Partial Translation of Reference 1

Jpn. Pat. Appln. KOKAI Publication No. 2002-055959

Filing No.: 2000-243787
Filing Date: August 11, 2000
Applicant: MACKPORT BIO-SECURITY CORP
Priority: Not Claimed
KOKAI Date: February 20, 2002
Request for Examination: Not filed
Int.Cl.: G06F 15/00
17/60
G09C 1/00
H04L 9/32

[A]
Column 14, Line 25 to Line 37

[0047] Further, in addition to the above aspect of the invention, according to another aspect of the invention, the information terminal includes a living body information registering means that registers living body information of a specific person for matching, a passport information storing means that stores passport information corresponding to the living body information registered in the living body information registering means, a living body information matching means for matching the living body information, in which a characteristic point is extracted by the characteristic point extracting means from the living body information read by the living body information reading means, with the living body information registered for matching in the living body information registering means, and an accessing means for taking out corresponding passport information from the passport information storing means and accessing a service site corresponding to the passport information when both pieces of the living body information match with each other as a result of the matching by the living body information matching means.

[B]
Column 19, Line 48 to Column 20, Line 27

[0080] A first one of the three patterns of configurations has a client terminal authentication type configuration as shown in FIG. 1. In this configuration, authentication is carried out in the inside of the client terminal 11 so an Internet passport is obtained. In a configuration of the memory area 16 of the client terminal authentication type, a living body information characteristic point data 20, such as fingerprint characteristic point data, exists in the RAM 17. Also, an Internet passport area 21 and a work area 22 exist together with the living body information characteristic point data 20. Among them, the Internet passport area 21 plays a role as the passport information storing means, and is not destroyed even when power is cut off.
[0081] In addition, the ROM 18 stores operation software 23, a characteristic point extraction algorithm 24, a living body information matching algorithm 25, and a key information storage section 26 that stores a secret key PC-B and a public key SS-A. Further, the living body information characteristic point data 20 registers living body information of a specific person for matching, and has a function as the living body

information registering means.
[0082] Among them, the operation software 23 is read first in the CPU 15 when the information terminal is turned on. The operation software 23 includes a high-order application and a low-order application.
[0083] In addition, the ROM 18 also stores the characteristic point extraction algorithm 24 as the characteristic point extracting means. The characteristic point extraction algorithm 24 extracts a characteristic point from living body information read by the living body information reading means 12. Then, the extracted characteristic point of the living body information is stored in the RAM 17 for matching in advance.

[C]
Column 22, Line 43 to Column 23, Line 22
[0098] In this state, the user accesses the specific service site 40 by using the client terminal 11 as shown in FIG. 4. Then, if the user desires to purchase a product, and view and download an information content in the service site 40. Then, the service site 40 side requests authentication with respect to the user, since there is the need for user authentication. In this case, for example, a Web screen of the service site 40 displays an "authentication button" and the like, and the user clicks the authentication button.
[0099] When the user clicks the authentication button on the Web screen, the client terminal 11 is in an authentication execution state. That is, the CPU 15 is in a state of controlling, for example, the operation software 23 to execute authentication. In this state, the CPU 15 notifies the living body information reading means 12 of a "living body information reading request". Then, the CPU 15 instructs the user to allow the living body information reading means 12 to read living body information through a displaying means and voice. An LED that displays the above instruction or a speaker emitting the voice may be provided separately. In addition, a similar instruction is issued to a high-order application through the interface 13. That is, the man-machine interface 13, such as a screen display of a personal computer and voice, is used to prompt the user to carry out reading operation of living body information.
[0100] Here, there are cases where a fingerprint information of quality of a certain standard cannot be obtained when dust and stain are attached on a surface of living body information such as a fingerprint, or on a surface of a scanner chip is stained in, for example, a fingerprint reading scanner. In such cases, reading of a fingerprint image is carried out until an image that satisfies quality of a certain standard is obtained.

[D]
Column 24, Line 17 to Column 25, Line 12
[0106] Here, when the pieces of living body information do not match with each other, the CPU 15 carries out display of "authentication is failed" and the like with respect to a high-order application through the interface 13 to notify the user. In contrast, when the pieces of living body information match with each other, the CPU 15 accesses the Internet passport area 21. Then, passport information can be obtained from the Internet passport area.
[0107] Details of the Internet passport area 21 will be described in a column of the Internet passport database 53 (of the second type) described later. Passport information is normally an ID or a passport for accessing the specific service site 40, or a card number of a settlement institution, such as a credit card company, a passport,

and the like. Hereinafter, description will be made by using the above information as the passport information.
[0108] In this case, the obtained passport information is transmitted from the client terminal 11 to the specific service site 40 in which the "authentication button" is clicked. The passport information of the specific service site 40 may be applied with encryption before being transmitted to the specific service site 40 as described later. Also, the system may be such that, in place of the passport information of the specific service site 40, other information (for example, authentication OK sign, or the like) may be applied with encryption and then transmitted. A case of applying encryption to the passport information of the specific service site 40 before transmission will be described in the description below.
[0109] When the client terminal 11 transmits the passport information of the specific service site 40 to the service site 40 site, an encryption processing function included in the operation software 23 applies encryption processing to the passport information. That is, an encrypting means is configured with the CPU 15, the operation software 23, the secret key PC-B, and the public key SS-A. In this encryption processing, the passport information (an ID and a passport, and the like) of the specific service site 40 is used as an original, and also one another copy of the same passport information is generated.
[0110] Then, the copy is compressed by using a hash function to create a digest version of the original. Then, a transmitter applies encryption to the digest version by using the own secret key PC-B. In this manner, the digest version becomes a digital signature. Further, the digital signature is attached to the original. When, both of the original and the attached digital signature are encrypted by using the public key SS-A on the service site 40 to conceal a transmission target. Then, after the above, the original and the digital signature are transmitted as encryption data to the service site 40 server side by SSL communication.

[E]
Column 27, Line 13 to Column 28, Line 41
[0123] Here, a configuration of data in the Web deposit 54 existing in the passport server 50 will be described based on FIG. 7 illustrated. Passport information shown in this figure is classified into levels described below based on access rights of the user. As shown in this figure, access rights of the user are classified into "Write permission right and deletion right", "Permission to know existence", "Permission to view content", "Permission to rewrite", "Permission to write once", and "Permission to use".
[0124] In addition, passport information of the user includes, for example, "Deposit ID", "Third-party institution description information", "Service site description information", "Public institution description information", "Private company description information", "User description information", "Living body information", and "Algorithm".
[0125] Access levels of the above passport information can be classified, for example, by setting flags. That is, a folder exclusively used, for example, for the deposit ID 30 is created, and a flag in property of the folder is set. For an access right to the deposit ID 30 being illustrated, the right of "Write permission right and deletion right" does not exist, and a flag corresponding to this right is set to "0". Also, since there is the right of "Permission to know existence", a flag corresponding to this right is set to "1".
[0126] In addition, in an another way of classifying access levels, a state capable of full access, in which all access rights are included, is shown by the number "0", and larger numbers are assigned as access rights are limited. In this case, numbers are

assigned for the number of combinations between columns from "Write permission right and deletion right" to "Permission to use" and rows from "Deposit ID" to "Algorithm", and access rights are corresponded to the numbers. In such a manner as well, control of access rights can be performed.

[0127] Since "Settlement institution information", "Service site information", and the like describe a plurality of pieces of settlement institution information and a plurality of pieces of service site information, folders for storing a plurality of pieces of information may be created and a flag is set for each of the folders.

[0128] As described above, as illustration of classifying access rights of the user, "o" shows permitted, "x" shows not permitted, and "Δ" shows permitted or not permitted depending on the principle of the service site 40. In this case, for "Deposit ID", "Write permission right and deletion right" is set to x, "Permitted to know existence" is set to o, "Permitted to view content" is set to o, "Permitted to rewrite" is set to x, "Permitted to write once" is set to x, and "Permitted to use" is set to o. In addition, for "Third-party institution description information", "Settlement institution information", "Service site description information", "Public institution description information", and "Private company description information", "Write permission right and deletion right" is set to o, "Permitted to know existence" is set to o, "Permitted to view content" is set to Δ, "Permitted to rewrite" is set to x, "Permitted to write once" is set to x, and "Permitted to use" is set to o.

[0129] Further, for "User description information", "Write permission right and deletion right" is set to o, "Permitted to know existence" is set to o, "Permitted to view content" is set to o, "Permitted to rewrite" is set to o, "Permitted to write once" is set to x, and "Permitted to use" is set to o. Also, for "Living body information", "Write permission right and deletion right" is set to x, "Permitted to know existence" is set to o, "Permitted to view content" is set to x, "Permitted to rewrite" is set to x, "Permitted to write once" is set to o, and "Permitted to use" is set to o. In addition, for "Algorithm", "Write permission right and deletion right" is set to x, "Permitted to know existence" is set to o, "Permitted to view content" is set to x, "Permitted to rewrite" is set to x, "Permitted to write once" is set to x, and "Permitted to use" is set to o.

[0130] However, setting of access rights is not limited to the ways in the above description, and an administrator of the Internet passport database 53 can set access rights in a variety of ways in consideration of importance of passport information.

[0131] When required passport information is pulled out to the passport server 50 from the deposit area configured as described above, the passport server 50 accesses a server of the specific service site 40 for which log-on is requested trough the accessing means 51 based on the passport information. Log-on to the specific service site 40 is carried out based on URL transmitted together with the passport information.

Ref1

対応なし、英抄

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号
特開2002－55959
（P2002－55959A）
(43)公開日　平成14年２月20日(2002.2.20)

(51)Int.Cl.⁷		識別記号	FI		テーマコード(参考)
Ｇ０６Ｆ	15/00	３３０	Ｇ０６Ｆ 15/00	３３０Ｆ	５Ｂ０４９
	17/60	２２２	17/60	２２２	５Ｂ０５５
		４１４		４１４	５Ｂ０８５
		５０４		５０４	５Ｊ１０４
		５１２		５１２	

審査請求　未請求　請求項の数30　ＯＬ　（全 23 頁）　最終頁に続く

(21)出願番号　特願2000－243787(P2000－243787)

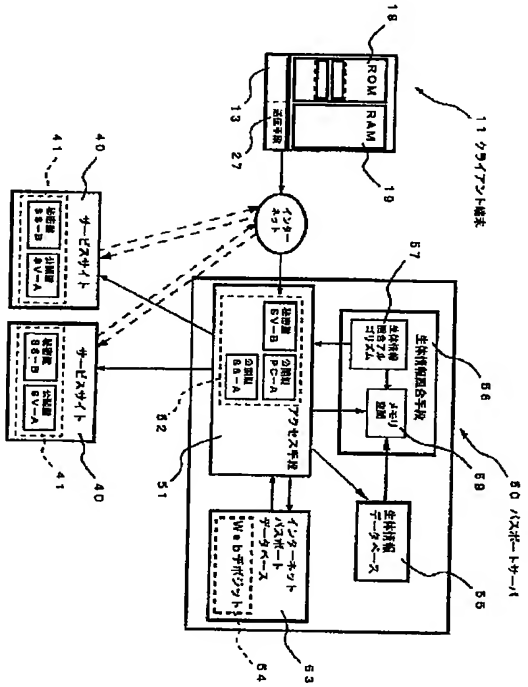
(22)出願日　平成12年８月11日(2000.8.11)

(71)出願人　500239937
株式会社マックポート・バイオセキュリティー
東京都品川区西大井６丁目11番14号
(72)発明者　中野　裕二
東京都品川区西大井６丁目11番14号
(74)代理人　100087859
弁理士　渡辺　秀治　（外１名）

最終頁に続く

(54)【発明の名称】　情報端末、認証システム及び認証方法

(57)【要約】
【課題】　生体情報を用いたシングルサインのみで、容易にかつ絶対的な特定人の認証を可能とすると共に、他人が不正に生体情報を利用し得ない、セキュリティの極めて高い認証システム及び認証方法を提供すること。
【解決手段】　ネットワークを介して特定人に係わる情報の管理を行い、その情報にアクセスする者が特定人か否かを認証する認証システム１０において、生体情報を読み取る生体情報読取手段１２と、特定人の生体情報を照合用として登録している生体情報登録手段５５と、生体情報登録手段５５と生体情報読取手段１２によって読み取られた生体情報との照合を行う生体情報照合手段５６と、生体情報登録手段に登録された生体情報と対応するように各サービスサイト４０のパスポート情報を記憶しているパスポート情報記憶手段５４と、生体情報が符合した場合にパスポート情報記憶手段５４から対応するパスポート情報を引き出して対応したサービスサイト４０にアクセスするアクセス手段５１と、を具備している。



1

【特許請求の範囲】

【請求項１】　ネットワークを介して特定人に係わる情報の管理を行い、その特定人に係わる情報にアクセスする者が特定人か否かを認証する認証システムにおいて、
生体情報を読み取る生体情報読取手段と、
特定人の生体情報を照合用として登録している生体情報登録手段と、
上記生体情報登録手段と上記生体情報読取手段によって読み取られた生体情報との照合を行う生体情報照合手段と、
上記生体情報登録手段に登録された生体情報と対応するように各サービスサイトの認証情報としてのパスポート情報を記憶しているパスポート情報記憶手段と、
上記生体情報照合手段によって登録された生体情報と、生体情報読取手段によって読み取られた生体情報とが符合した場合に、上記パスポート情報記憶手段から対応するパスポート情報を引き出し、このパスポート情報に対応したサービスサイトにアクセスするアクセス手段と、
を具備することを特徴とする認証システム。

【請求項２】　前記生体情報読取手段によって読み取られ、前記生体情報照合手段との照合が為される生体情報を記憶するための読取生体情報記憶部が設けられると共に、この読取生体情報記憶部に記憶されている生体情報と同一の生体情報が生体情報読取手段から読み取られた場合に、生体情報照合手段での生体情報の照合を行わないようにする照合回避手段が設けられていることを特徴とする請求項１記載の認証システム。

【請求項３】　前記読取生体情報記憶部、及び照合回避手段はパスポートサーバ内に設けられていることを特徴とする請求項２記載の認証システム。

【請求項４】　前記読取生体情報記憶部、及び照合回避手段は情報端末内に設けられていることを特徴とする請求項２記載の認証システム。

【請求項５】　前記生体情報登録手段、生体情報照合手段、パスポート情報記憶手段及びアクセス手段はパスポートサーバ内に設けられていることを特徴とする請求項１から４のいずれか１項に記載の認証システム。

【請求項６】　前記生体情報読取手段は情報端末内に設けられていると共に、この生体情報読取手段によって読み取られた生体情報は、情報端末内の送信手段によってパスポートサーバに伝送されることを特徴とする請求項５記載の認証システム。

【請求項７】　前記情報端末は、前記生体情報読取手段によって読み取られた生体情報のデータ処理を行うデータ処理手段と、
このデータ処理手段によってデータ処理が為された生体情報から特徴点を抽出する特徴点抽出手段と、
前記パスポートサーバの公開鍵、及び独自の秘密鍵を記憶している鍵情報記憶部と、
上記特徴点抽出手段によって特徴点が抽出された生体情報を、鍵情報記憶部に記憶されている独自の秘密鍵で暗号化するとともに、その後にパスポートサーバの公開鍵で暗号化するための暗号化手段と、
を具備することを特徴とする請求項６記載の認証システム。

2

【請求項８】　前記生体情報が前記生体情報登録手段に登録されるに際して識別情報が割り当てられると共に、この識別情報は識別情報記憶部に記憶されており、前記生体情報照合手段での生体情報の照合を行うに先立って識別情報によって前記生体情報登録手段に登録されている生体情報を特定することを特徴とする請求項１から７のいずれか１項に記載の認証システム。

【請求項９】　前記識別情報記憶部は前記情報端末内部に設けられていることを特徴とする請求項８記載の認証システム。

【請求項１０】　前記識別情報記憶部は前記情報端末内部に設けられていると共に、この識別情報記憶部に記憶されている識別情報は、前記生体情報と共に請求項４記載の暗号化手段によって暗号化されることを特徴とする請求項８記載の認証システム。

【請求項１１】　前記パスポート情報記憶手段は、アクセスレベル別に分類されていることを特徴とする請求項１から１０のいずれか１項に記載の認証システム。

【請求項１２】　前記パスポート情報記憶手段のアクセスレベルは、パスポート情報に関するデータの書込みや削除を行えるレベルと、パスポート情報に関するデータの存在を知ることができるレベルと、パスポート情報に関するデータの内容を見ることができるレベルと、パスポート情報に関するデータの書換えが行えるレベルと、パスポート情報に関するデータのワンタイムの書込みができるレベルと、パスポート情報に関するデータの利用ができるレベルに分類されていることを特徴とする請求項１１記載の認証システム。

【請求項１３】　前記アクセスレベルの設定は、フラグの設定によって行うことを特徴とする請求項１１又は１２記載の認証システム。

【請求項１４】　前記アクセスレベルの設定は、アクセスレベル別に割り当てられた数字の設定によって行うことを特徴とする請求項１１又は１２記載の認証システム。

【請求項１５】　前記パスポート情報記憶手段には、パスポート情報に対応したサービスサイトのＵＲＬも記憶されており、前記生体情報登録手段に登録された生体情報と、生体情報読取手段によって読み取られた生体情報とが符合した場合に、前記パスポート情報記憶手段から対応するパスポート情報と共にサービスサイトのＵＲＬも引き出し、このＵＲＬに基づいて前記アクセス手段で該サービスサイトにアクセスすることを特徴とする請求項１から１４のいずれか１項に記載の認証システム。

【請求項１６】　前記生体情報読取手段には、読み取ら

れた生体情報が基準の品質以下の場合に再度生体情報の読み取りを行うようにする生体情報判別手段が設けられていることを特徴とする請求項１から１５のいずれか１項に記載の認証システム。

【請求項１７】　ネットワークを介してパスポートサーバにアクセスすることが可能な情報端末において、
生体情報を読み取る生体情報読取手段と、
上記生体情報読取手段によって読み取られた生体情報のデータ処理を行うデータ処理手段と、
上記データ処理手段によってデータ処理が為された生体情報から特徴点を抽出する特徴点抽出手段と、
パスポートサーバの公開鍵、及び独自の秘密鍵を記憶している鍵情報記憶部と、
上記特徴点抽出手段によって特徴点が抽出された生体情報を、鍵情報記憶部に記憶されている独自の秘密鍵で暗号化するとともに、その後にパスポートサーバの公開鍵で暗号化するための暗号化手段と、
上記暗号化手段によって暗号化された生体情報をパスポートサーバ側に送信するための送信手段と、
を具備することを特徴とする情報端末。

【請求項１８】　前記情報端末は、
特定人の生体情報を照合用として登録している生体情報登録手段と、
上記生体情報登録手段に登録された生体情報に対応するパスポート情報を記憶しているパスポート情報記憶手段と、
前記生体情報読取手段によって読み取られ前記特徴点抽出手段によって特徴点が抽出された生体情報と生体情報登録手段に照合用として登録されている生体情報との照合を行うための生体情報照合手段と、
上記生体情報照合手段での照合の結果、生体情報が符合した場合に上記パスポート情報記憶手段から対応するパスポート情報を引き出し、このパスポート情報に対応したサービスサイトにアクセスするアクセス手段と、
を具備することを特徴とする請求項１７記載の情報端末。

【請求項１９】　前記情報端末は、
特定人の生体情報を照合用として登録している生体情報登録手段と、
前記生体情報読取手段によって読み取られ前記特徴点抽出手段によって特徴点が抽出された生体情報と生体情報登録手段に照合用として登録されている生体情報との照合を行うための生体情報照合手段と、
を具備していて、上記生体情報照合手段での照合の結果、生体情報が符合した場合に符合情報を前記暗号化手段で前記生体情報に代えて暗号化し、この暗号化された生体情報を送信手段で送信することを特徴とする請求項１７記載の情報端末。

【請求項２０】　前記情報端末には、この情報端末独自の識別情報が割り当てられていて、前記生体情報読取手段で読み取られた生体情報を伝送手段で伝送するに際して識別情報も伝送することを特徴とする請求項１７記載の情報端末。

【請求項２１】　前記生体情報読取手段によって読み取られた生体情報を記憶するための読取生体情報記憶部が設けられると共に、この読取生体情報記憶部に記憶されている生体情報と同一の生体情報が生体情報読取手段から読み取られた場合に、前記送信手段から生体情報の送信を行わないようにする送信回避手段が設けられていることを特徴とする請求項１７から２０のいずれか１項に記載の情報端末。

【請求項２２】　前記生体情報読取手段には、読み取られた生体情報が基準の品質以下の場合に再度生体情報の読み取りを行うようにする生体情報判別手段が設けられていることを特徴とする請求項１７から２１のいずれか１項に記載の情報端末。

【請求項２３】　ネットワークを介して特定人に係わる情報の管理を行い、その特定人に係わる情報にアクセスする者が特定人か否かを認証する認証方法において、
生体情報を読み取る生体情報読取工程と、
特定人の生体情報を照合用として登録している生体情報照合手段の生体情報と、上記生体情報読取工程によって読み取られた生体情報との照合を行う生体情報照合工程と、
上記生体情報照合工程によって生体情報が符合した場合、この生体情報に対応するようにパスポート情報記憶手段に記憶されているパスポート情報を得るパスポート情報取得工程と、
上記パスポート情報取得工程によって得られたパスポート情報に基づき、このパスポート情報に対応したサービスサイトにアクセスして該サービスサイトでのログオンを行うアクセス工程と、
を具備することを特徴とする認証方法。

【請求項２４】　前記生体情報照合工程での生体情報の照合に先立って、照合用として登録している特定人の生体情報を識別情報に基づいて検索する識別手段検索工程を具備していることを特徴とする請求項２３記載の認証方法。

【請求項２５】　前記生体情報登録工程、生体情報照合工程、パスポート情報記憶工程及びアクセス工程はパスポートサーバ内で行われることを特徴とする請求項２３又は２４記載の認証方法。

【請求項２６】　前記生体情報読取工程は情報端末内で行われると共に、この生体情報読取工程によって読み取られた生体情報は、情報端末内で行われる送信工程によってパスポートサーバ内に伝送されることを特徴とする請求項２５記載の認証方法。

【請求項２７】　前記生体情報読取工程で読み取られた生体情報に対して、前記生体情報照合工程に先立って、前記生体情報読取手段によって読み取られた生体情報の

データ処理を行うデータ処理工程と、
上記データ処理工程によってデータ処理が為された生体情報から特徴点を抽出する特徴点抽出工程と、
上記特徴点抽出工程によって特徴点が抽出された生体情報を、前記パスポートサーバの鍵情報記憶部に記憶されている独自の秘密鍵で暗号化するとともに、その後にパスポートサーバの鍵情報記憶部に記憶されている公開鍵で暗号化する暗号化工程と、
を具備する請求項２６記載の認証方法。

【請求項２８】　前記パスポート情報取得工程により得られるパスポート情報は、前記パスポート情報記憶手段内部においてアクセスレベルに分類されて記憶されていることを特徴とする請求項２３から２７のいずれか１項に記載の認証方法。

【請求項２９】　前記パスポート情報取得工程により得られるパスポート情報の前記パスポート情報記憶手段内部におけるアクセスレベルは、パスポート情報に関するデータの書込みや削除を行えるレベルと、パスポート情報に関するデータの存在を知ることができるレベルと、パスポート情報に関するデータの内容を見ることができるレベルと、パスポート情報に関するデータの書換えが行えるレベルと、パスポート情報に関するデータのワンタイムの書込みができるレベルと、パスポート情報に関するデータの利用ができるレベルに分類されていることを特徴とする請求項２８記載の認証方法。

【請求項３０】　前記パスポート情報取得工程において、前記パスポート情報記憶手段にパスポート情報と共にこのパスポート情報に対応したＵＲＬも記憶されており、前記生体情報照合工程において生体情報が符合した場合に、前記パスポート情報記憶手段から対応するパスポート情報と共にサービスサイトのＵＲＬも引き出し、このＵＲＬに基づいて前記アクセス手段で該サービスサイトにアクセスすることを特徴とする請求項２３から２９のいずれか１項に記載の認証方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、生体情報を利用した認証システム及び認証方法に関する。

【０００２】

【従来の技術】現在、個人の信用において商取引を行う場合には、その個人の認証を行うために種々の手段（トークン）を用いている。例えば、クレジットカードにおいては、暗証番号を用いたり、或いはサイン等を用いてカード使用者が本人であるか否かの確認を行っている。

【０００３】現在、個人の身分を証明する場合、身分証明を提示する場によって、リアル世界の身分証明手段、準バーチャル世界の身分証明手段、及びバーチャル世界の身分証明手段の三段階に分けられる。このうち、リアル世界における身分証明手段とは、従前から存在する身分証明手段であり、基本的には身分証明手段を有する個人を対面にて身分照合するものである。

【０００４】このリアル世界の身分証明手段としては、例えば学生であれば学生証、会社員であれば社員証、車の運転を行う人の場合には運転免許証、海外旅行を行う人の場合にはパスポート等がある。さらに、他にはクレジット決済を行う人の場合はクレジットカードとサイン、或いは病院に通院する場合に必要な健康保険証、さらには各種会員証、ポイントカード等がある。

【０００５】また、準バーチャル世界の身分証明手段とは、所定の箇所に存する端末からオンラインを介して身分照合を行うものである。この準バーチャル世界の身分証明手段としては、銀行のＡＴＭにおいて銀行のキャッシュカードとパスワードによるものがある。さらに、バーチャル世界の身分証明手段とは、近年急速に普及したインターネット等のネットワークを介しての身分照合を行うものである。バーチャル世界の身分証明手段としては、インターネット接続のプロバイダーにおける会員ＩＤとパスワード、会社のパソコンにおけるＩＤとパスワード、ショッピングモールにおける会員ＩＤとパスワードがある。また、他には、ＰＫＩ（Public Key Infrastructure）技術を適用した身分証明手段もある。

【０００６】

【発明が解決しようとする課題】ところで、リアル世界の身分証明手段では、持ち物による所有者認証、顔写真による目視認証を行い、またクレジットカードにおいてはサイン癖による目視認証を行っている。すなわち、個人と個人とが対面するため、かかる身分証明手段で混乱のない商取引が実現されている。かかるリアル世界で身分を偽装するためには、（１）偽造組織（人）、（２）偽造技術、（３）資本、（４）費用対効果、（５）他人の身分証明手段を複写し、それを短時間で利用する高度なビジネスモデル、の夫々が必要とされる。また、身分証明手段を偽造できたとしても、身分証明手段の利用箇所に監視カメラが設置されている場合が多く、かかる監視カメラでの録画により、例え不正を行ったとしても後日録画内容を検索することができる。それ故、リアル世界では、偽装が困難であり、よって現状の身分証明手段で混乱のない商取引が実現されている。

【０００７】また、準バーチャル世界の身分証明手段では、例えばキャッシュカードとパスワードにより認証を行っている。この場合、キャッシュカードという持ち物、及びパスワードの記憶の二つの手段により、本人か否かの認証を行っている。それ故、パスワードを忘れてしまうと該キャッシュカードが利用できなくなる、といった問題を有している。

【０００８】また、パスワードを盗まれた場合には、キャッシュカードを盗むだけで簡単に特定人に成りすますことが可能となる。さらに、特に複数のキャッシュカードを持った場合に顕著であるが、パスワードは忘れやすいものである故、パスワードを特定人の個人属性（例え

ば誕生日等）にして記憶している場合が多い。それ故、他人は特定人のパスワードを容易に推測できる場合が多い。しかしながら、準バーチャル世界においても、例えばＡＴＭの設置箇所には監視カメラが設置されている場合がほとんどであり、偽装しても後日録画内容を検索することが可能である。

【０００９】また、バーチャル世界の身分証明手段では、インターネット等のネットワークを介して特定人か否かの認証を行うことが必要とされる。かかるインターネットにおいては、対面でないため顔を確かめることができない。また、監視カメラで撮影することもできない。さらには、インターネットにおいては匿名で活動することが許されている。それ故、相手方がどこに住んでいるかさえも分からない、といった問題を有している。

【００１０】このようなバーチャル世界の身分証明手段では、例えばＩＤとパスワードにより認証する場合、或いはＰＫＩの秘密鍵を保持しこれを用いて認証する場合がある。しかしながら、ＩＤとパスワードにより認証する場合、ＩＤやパスワードを忘れてしまうと利用できない、といった問題を有している。それ故、パスワードを個人属性にすることが多く、他人が容易にパスワードを推測することができる、といった準バーチャル世界と同様の問題を有している。また、ＩＤやパスワードが盗まれると、簡単に他人が特定人に成りすますことができる。

【００１１】さらに、ＰＫＩの秘密鍵を用いて認証する場合、この秘密鍵が他人に盗まれると成りすましが防止できない、といった問題を有している。すなわち、ＰＫＩを特定の記憶メディアや情報端末に保存した場合、この秘密鍵が盗まれると、公開鍵により暗号化されたデータが容易に復号化されてしまう。また、秘密鍵により暗号化してデータを送信し、受信した相手の公開鍵で復号化すると、データが誰から送られてきたのかを認証することができるが、厳密に言えば、秘密鍵を保存している記憶メディアや情報端末を認証するのみである。それ故、他人が秘密鍵を不正に入手した場合には、特定人に成りすますことが可能となってしまう。すなわち、特定人であることの絶対的な認証は、ＰＫＩ方式では行えない。

【００１２】さらに、バーチャル世界では、リアル世界及び準バーチャル世界のように監視カメラで録画することがないため、他人が特定人に成りすます場合のリスクが、リアル世界及び準バーチャル世界と比較して非常に高いものとなっている。

【００１３】特に近年は、インターネットの急速な発展・普及により、インターネットを介したオンラインショッピング等の電子商取引が徐々に活発化するようになってきている。かかる電子商取引においては、本人であるか否かを確実に認証する必要がある。しかしながら、電子商取引の現状においては、例えばクレジットカードのカード番号と暗証番号を確認することにより、本人であるか否かの認証を行っている。このため、かかるカード番号や暗証番号が他人に知られた場合、成りすましを防ぐことができず、リスクの高い商取引手段とならざるを得ないのが現状である。また、このような認証事故によるリスクを回避するために、クレジットカード会社等の債権回収業者は、保険会社との契約を行うのが通常である。かかる保険契約では、認証事故の頻度がリアル世界と比較して大きいため、保険料が高額となり、これが価格低下の妨げとなっている。

【００１４】また、電子商取引以外にも、例えば行政庁・各役所に対する手続をインターネットを介して行えるようにする、いわゆる電子政府の構想があり、例えばシンガポールのように、既に実用段階に踏み切っている国も存在する。また、我が国も、２００３年度に電子政府の実現へ向けて準備を進めている。このような電子政府構想においても、特定人であるか否かを確実に認証する必要があり、かかる特定人であることの認証が確実に為されないと、他人がプライバシーを侵害してしまったり、個人の財産・権利等に係わる問題を生じてしまう場合がある。このため、日本においては、現状ではまだ実用化がなされていなく、一部で実験的に導入されているのみである。

【００１５】以上のことをまとめると、図８のようになる。この図に示すように、バーチャル世界においての特定人か否かの認証は、記憶手段に記憶された情報に基づく認証である。ここで、例えばＩＣカードのようなハードウエア手段を所持している所持者が真の所有者であるか否かの確認は行えなく、またハードウエア手段が偽造されたものであるか否かの真偽を確認することができない。よって、最終的にはソフトウエアのみで行う必要がある。さらに、かかるソフトウエアによる認証において、認証事故がなく精度良く行えるようにする必要がある。

【００１６】上述のような特定人であるか否かの認証が確実に行われるようになれば、インターネットを介しての電子商取引、或いは電子政府構想が一般化・現実化するものとなり、かかる認証を行える認証システム、認証方法が待望されている。また、その認証が複雑でなく、誰でも行えるように簡便化されるものが待望されている。

【００１７】本発明は、上記の事情に基づきなされたもので、その目的とするところは、生体情報を用いたシングルサインのみで、容易にかつ絶対的な特定人の認証を可能とすると共に、他人が不正に生体情報を利用し得ない、セキュリティの極めて高い認証システム及び認証方法を提供しよう、とするものである。

【００１８】

【課題を解決するための手段】上述の目的を達成するため、本発明は、ネットワークを介して特定人に係わる情

報の管理を行い、その特定人に係わる情報にアクセスする者が特定人か否かを認証する認証システムにおいて、生体情報を読み取る生体情報読取手段と、特定人の生体情報を照合用として登録している生体情報登録手段と、生体情報登録手段と生体情報読取手段によって読み取られた生体情報との照合を行う生体情報照合手段と、生体情報登録手段に登録された生体情報と対応するように各サービスサイトの認証情報としてのパスポート情報を記憶しているパスポート情報記憶手段と、生体情報照合手段によって登録された生体情報と、生体情報読取手段によって読み取られた生体情報とが符合した場合に、パスポート情報記憶手段から対応するパスポート情報を引き出し、このパスポート情報に対応したサービスサイトにアクセスするアクセス手段と、を具備することとしたものである。

【００１９】このため、生体情報を生体情報読取手段で読み取り、特定人の生体情報と符合すれば、パスポート情報記憶手段に記憶されているパスポート情報を引き出して、アクセス手段によってこのパスポート情報に対応したサービスサイトにアクセスすることが可能となる。すなわち、生体情報の読み取りのみによって所定のサービスサイトにアクセス可能となり、複数のサービスサイトのＩＤやパスワードに対応させることができる。このため、一々複数のＩＤやパスワードを覚える必要がなく、利便性を向上させることが可能となる。すなわち、生体情報をシングルサイン感覚で読み取らせ、それに基づいた種々のサービスサイトの認証を行うことが可能となる。すなわち、ユーザは生体情報を自己の身分証明手段として用いるのみで、各サービスサイトでの認証を行うことが可能となる。

【００２０】また、他の発明は、上述の発明に加えて更に、生体情報読取手段によって読み取られ、生体情報照合手段との照合が為される生体情報を記憶するための読取生体情報記憶部が設けられると共に、この読取生体情報記憶部に記憶されている生体情報と同一の生体情報が生体情報読取手段から読み取られた場合に、生体情報照合手段での生体情報の照合を行わないようにする照合回避手段が設けられていることとしたものである。

【００２１】このため、一度読み取られた生体情報を読取生体情報記憶部に記憶させておき、この読取生体情報記憶部に記憶されている生体情報と同一の生体情報に基づく照合を、照合回避手段で拒否することができる。すなわち、他人が不正に特定人の生体情報を入手した場合、その生体情報を用いて生体情報の照合を行おうとしても、読取生体情報記憶部に記憶されている生体情報を用いることはできない。これは、例えば指紋のような生体情報では、押圧角度や押圧面積、或いは押圧力が同じである全く同一の生体情報が得られることはほとんどないことに基づくものである。

【００２２】さらに、他の発明は、上述の発明に加えて更に、読取生体情報記憶部、及び照合回避手段はパスポートサーバ内に設けられていることとしたものである。このため、パスポートサーバにおいて一度照合した生体情報を蓄えておくことができ、この蓄えられた生体情報と同一の生体情報がパスポートサーバに送信されてきた場合には、照合回避手段で生体情報の照合を回避することが可能となる。

【００２３】また、他の発明は、上述の発明に加えて更に、読取生体情報記憶部、及び照合回避手段は情報端末内に設けられることとしたものである。このため、情報端末内部に一度照合した生体情報を蓄えておくことができ、この蓄えられた生体情報と同一の生体情報が生体情報読取手段で読み取られた場合には、照合回避手段で生体情報の照合を回避することが可能となる。すなわち、クライアント端末側で、照合回避手段を働かせることが可能となる。

【００２４】さらに、他の発明は、生体情報登録手段、生体情報照合手段、パスポート情報記憶手段及びアクセス手段はパスポートサーバ内に設けられていることとしたものである。

【００２５】このため、同一のパスポートサーバ内で、生体情報の照合や、それに対応したパスポート情報を引き出してアクセス手段でサービスサイトにアクセスする。それにより、アクセス速度を速くすることが可能となる。

【００２６】また、他の発明は、生体情報読取手段は情報端末内に設けられていると共に、この生体情報読取手段によって読み取られた生体情報は、情報端末内の送信手段によってパスポートサーバに伝送されることとしたものである。

【００２７】このため、情報端末単独で生体情報の読み取りを行い、この情報端末によって読み取られた生体情報を情報端末内の送信手段によって伝送する。それにより、ユーザが所持可能な情報端末を用いてネットワークを介して簡易に生体情報による認証を行い、この生体情報とパスポート情報を対応させることで、生体情報をシングルサイン感覚で簡易に身分証明手段として用いることが可能となる。

【００２８】さらに、他の発明は、情報端末は、生体情報読取手段によって読み取られた生体情報のデータ処理を行うデータ処理手段と、このデータ処理手段によってデータ処理が為された生体情報から特徴点を抽出する特徴点抽出手段と、パスポートサーバの公開鍵、及び独自の秘密鍵を記憶している鍵情報記憶部と、特徴点抽出手段によって特徴点が抽出された生体情報を、鍵情報記憶部に記憶されている独自の秘密鍵で暗号化するとともに、その後にパスポートサーバの公開鍵で暗号化するための暗号化手段と、を具備することとしたものである。

【００２９】このため、生体情報読取手段によって読み取られた生体情報を、まずデータ処理手段によるデータ

処理を行う。続いて、データ処理手段でデータ処理が為された生体情報に対して、特徴点抽出手段で特徴点の抽出を行う。そして、特徴点が抽出された生体情報に対して、暗号化手段を用いて鍵情報記憶部に記憶されている独自の秘密鍵で暗号化した後に、パスポートサーバの公開鍵で暗号化を行う。このような状態でパスポートサーバ側に伝送すれば、例え伝送経路の途中で他人が不正に生体情報を入手しても、秘密鍵及び公開鍵で暗号化が為されているので、解読が極めて困難なものとなり、生体情報の伝送に際しての安全性を確保することが可能となる。また、情報端末独自の秘密鍵で暗号化した後に、パスポートサーバ側の公開鍵で暗号化するので、伝送経路の途中で他人が不正に生体情報を入手し、入手した生体情報に基づいて改ざんを加えて他人が特定人に成りすまそうとしても、逆関数のないハッシュ関数の性質から、改ざんしたか否かを容易に検知することが可能となる。すなわち、事実上、特定人に成りすますことが不可能となる。

【００３０】また、他の発明は、上述の各発明に加えて更に、生体情報が生体情報登録手段に登録されるに際して識別情報が割り当てられると共に、この識別情報は識別情報記憶部に記憶されており、生体情報照合手段での生体情報の照合を行うに先立って識別情報によって生体情報登録手段に登録されている生体情報を特定することとしたものである。

【００３１】このため、生体情報照合手段での照合を行うに先立って、識別情報に基づいて生体情報登録手段に登録されている生体情報を引き出すことが可能となる。すなわち、かかる識別情報での生体情報の検索を行うことによって、生体情報の照合を行う際の時間の短縮を図ることが可能となる。

【００３２】さらに、他の発明は、上述の発明に加えて更に、識別情報記憶部は前記情報端末内部に設けられていることとしたものである。このため、情報端末で生体情報の読み取りを行い、この生体情報を情報端末から伝送するに際して、識別情報を識別情報記憶から呼び出して一緒に伝送することとなる。このように、識別情報記憶部を情報端末に設けることで、一々特定人が識別情報を入力しなくても、生体情報の読取を行えば、この生体情報の読み取りと共に生体情報の伝送を行うことが可能となる。

【００３３】また、他の発明は、上述の発明に加えて更に、識別情報記憶部は情報端末内部に設けられていると共に、この識別情報記憶部に記憶されている識別情報は、生体情報と共に暗号化手段によって暗号化されることとしたものである。

【００３４】このため、生体情報のみならず、識別情報を他人が不正に伝送経路途中で入手しても、その内容を秘匿化することが可能となり、識別情報の解読が極めて困難となって安全性を確保することが可能となる。また、識別情報に対しても情報端末独自の秘密鍵で暗号化した後に、パスポートサーバ側の公開鍵で暗号化するので、伝送経路の途中で他人が不正に識別情報を入手し、入手した識別情報に基づいて改ざんを加えて他人が特定人に成りすまそうとしても、逆関数のないハッシュ関数の性質から、改ざんしたか否かを容易に検知することが可能となる。すなわち、事実上、特定人に成りすますことが不可能となる。

【００３５】さらに、他の発明は、上述の各発明に加えて更に、パスポート情報記憶手段は、アクセスレベル別に分類されていることとしたものである。この場合、パスポート情報は、生体情報と対応するように設けられているので、生体情報読取手段によって生体情報を読み取らせると、この生体情報に対応したパスポート情報を引き出すことができる。この場合、ＩＤやパスワードの如き単なる情報ではなく、生体情報を自己の身分証明手段として用いて認証を行うため、他人が特定人に成りすますのを防止することができる。

【００３６】さらにユーザのアクセスレベルの設定により、ネットを介しての会員制サービスサイト、或いは決済機関、公的機関、民間企業等が運営する、種々のサービスサイトにメリットが生ずることとなる。例えば、決済機関の情報を記載している場合、ユーザのアクセスレベルを「存在を知ることができる」を○として、「書換えできる」を×とした場合、ユーザは勝手にパスポート情報であるＩＤやパスワードを書き換えることができない。このようなアクセスレベルの設定により、各サイト側において生体情報を活用した本人の絶対認証を現実的に利用可能となる。

【００３７】また、例えばデータを保存する領域をパスポート情報記憶手段内に設けた場合、アクセスレベルの設定の仕方によってはデータの保存はできるがコピーはできないようにすることもできる。この場合には、特定人は生体情報を用いてアクセス可能となり、パスポート情報記憶手段内でそのデータをアクセスレベルに設定されたレベル内で利用可能となるが、違法なコピー等は行えないものとなる。それによって、種々のコンテンツからデータを該パスポート情報記憶手段内にダウンロードした場合、他の領域にはコピーできないため、該データの著作権を守ることが可能となる。

【００３８】また、他の発明は、上述の発明に加えて更に、パスポート情報記憶手段のアクセスレベルは、パスポート情報に関するデータの書込みや削除を行えるレベルと、パスポート情報に関するデータの存在を知ることができるレベルと、パスポート情報に関するデータの内容を見ることができるレベルと、パスポート情報に関するデータの書換えが行えるレベルと、パスポート情報に関するデータのワンタイムの書込みができるレベルと、パスポート情報に関するデータの利用ができるレベルに分類されていることとしたものである。

【００３９】このように各レベルに分けて分類したことにより、夫々のサービスサイトが要求する状態に、ユーザのアクセス権利を制限することが可能となる。これによって、生体情報の読み取りで該パスポート情報記憶手段にアクセスした場合、ユーザに対してもＩＤやパスワードの秘匿性を確保することも可能となる。

【００４０】さらに、他の発明は、上述の各発明に加えて更に、アクセスレベルの設定は、フラグの設定によって行うこととしたものである。このようにフラグの設定によりアクセスレベルを種々設定するので、簡易な操作でサービスサイト側の希望に沿ったアクセスレベルにパスポート情報記憶手段を設定できる。

【００４１】また、他の発明は、上述の各発明に加えて更に、アクセスレベルの設定は、アクセスレベル別に割り当てられた数字の設定によって行うこととしたものである。このようにアクセスレベル別に割り当てられた数字の設定によってアクセスレベルを種々設定するので、簡易な操作でサービスサイト側の希望に沿ったアクセスレベルにパスポート情報記憶手段を設定することができる。

【００４２】さらに、他の発明は、上述の各発明に加えて更に、パスポート情報記憶手段には、パスポート情報に対応したサービスサイトのＵＲＬも記憶されており、生体情報登録手段に登録された生体情報と、生体情報読取手段によって読み取られた生体情報とが符合した場合に、パスポート情報記憶手段から対応するパスポート情報と共にサービスサイトのＵＲＬも引き出し、このＵＲＬに基づいてアクセス手段で該サービスサイトにアクセスすることとしたものである。

【００４３】このため、生体情報照合手段での照合で生体情報が符合した場合、パスポート情報記憶手段から対応するパスポート情報と共にサービスサイトのＵＲＬを引き出して、このＵＲＬに基づいてアクセス手段で特定のサービスサイトにアクセスすることが可能となる。すなわち、一々ＵＲＬを検索したり入力せずに、特定のサービスサイトにアクセス可能となる。

【００４４】また、他の発明は、上述の発明に加えて更に、生体情報読取手段には、読み取られた生体情報が基準の品質以下の場合に再度生体情報の読み取りを行うようにする生体情報判別手段が設けられていることとしたものである。このため、生体情報により特定人か否かの照合を行う場合、基準の品質以上の生体情報にて特定人か否かの認証を行える。それによって、例えば生体情報読取手段の汚れによって一定基準以下の生体情報に基づく認証を行うのを防止することができ、認証精度の向上を図ることができる。

【００４５】また、他の発明は、ネットワークを介してパスポートサーバにアクセスすることが可能な情報端末において、生体情報を読み取る生体情報読取手段と、生体情報読取手段によって読み取られた生体情報のデータ処理を行うデータ処理手段と、データ処理手段によってデータ処理が為された生体情報から特徴点を抽出する特徴点抽出手段と、パスポートサーバの公開鍵、及び独自の秘密鍵を記憶している鍵情報記憶部と、特徴点抽出手段によって特徴点が抽出された生体情報を、鍵情報記憶部に記憶されている独自の秘密鍵で暗号化するとともに、その後にパスポートサーバの公開で暗号化するための暗号化手段と、暗号化手段によって暗号化された生体情報をパスポートサーバ側に送信するための送信手段と、を具備することとしたものである。

【００４６】このように、生体情報読取手段によって読み取られた生体情報をデータ処理手段及び特徴点抽出手段を介して特徴点の抽出を行う。さらに、特徴点の抽出が為された生体情報に対して暗号化手段により独自の秘密鍵、及びパスポートサーバの公開鍵で暗号化する。すなわち、本人であるか否かの絶対的な認証を行える生体情報を用い、さらにこの生体情報に対して、どの情報端末から送信されたかを特定するための秘密鍵で暗号化する。そのため、特定人を生体情報で特定可能であると共に、秘密鍵によって端末認証も行える。さらに、生体情報を秘密鍵で暗号化した後に、パスポートサーバの公開鍵で暗号化を行うので、秘密鍵を有しているパスポートサーバのみしか復号化を行えない。それによって、生体情報の秘匿性を保つことが可能となる。

【００４７】さらに、他の発明は、上述の発明に加えて更に、情報端末は、特定人の生体情報を照合用として登録している生体情報登録手段と、生体情報登録手段に登録された生体情報に対応するパスポート情報を記憶しているパスポート情報記憶手段と、生体情報読取手段によって読み取られ特徴点抽出手段によって特徴点が抽出された生体情報と生体情報登録手段に照合用として登録されている生体情報との照合を行うための生体情報照合手段と、生体情報照合手段での照合の結果、生体情報が符合した場合にパスポート情報記憶手段から対応するパスポート情報を引き出し、このパスポート情報に対応したサービスサイトにアクセスするアクセス手段と、を具備することとしたものである。

【００４８】このため、生体情報読取手段によって読み取らせた生体情報を、生体情報照合手段によって照合することが可能となる。すなわち、情報端末側で特定人か否かの認証が行える、クライアント端末認証型の情報端末にすることができる。さらに、生体情報が照合した場合に、パスポート情報記憶手段から対応するパスポート情報を引き出して、このパスポート情報に対応したサービスサイトにアクセス手段でアクセスすることができる。このようにすることで、情報端末側において各サービスサイトでの認証を行って、該サービスサイトにログオンすることが可能となる。

【００４９】また、他の発明は、上述の発明に加えて更に、情報端末は、特定人の生体情報を照合用として登録

している生体情報登録手段と、生体情報読取手段によって読み取られ特徴点抽出手段によって特徴点が抽出された生体情報と生体情報登録手段に照合用として登録されている生体情報との照合を行うための生体情報照合手段と、を具備していて、生体情報照合手段での照合の結果、生体情報が符合した場合に符合情報を暗号化手段で生体情報に代えて暗号化し、この暗号化された生体情報を送信手段で送信することとしたものである。

【００５０】このため、生体情報読取手段で読み取らせた生体情報に基づいて、特定人であるか否かの認証を生体情報照合手段で情報端末側で行うことが可能となる。また、特定人であるとの認証が為された場合、符合情報を暗号化手段で暗号化した後に送信手段で送信するので、符合情報の安全性、秘匿性を確保することが可能となる。

【００５１】さらに、他の発明は、上述の発明に加えて更に、情報端末には、この情報端末独自の識別情報が割り当てられていて、生体情報読取手段で読み取られた生体情報を伝送手段で伝送するに際して識別情報も伝送することとしたものである。

【００５２】このため、パスポートサーバ側において生体情報照合手段での照合を行うに先立って、識別情報に基づいて生体情報登録手段に登録されている生体情報を引き出すことが可能となる。すなわち、かかる識別情報での生体情報の検索を行うことによって、生体情報の照合を行う際の時間の短縮を図ることが可能となる。

【００５３】また、他の発明は、上述の各発明に加えて更に、生体情報読取手段によって読み取られた生体情報を記憶するための読取生体情報記憶部が設けられると共に、この読取生体情報記憶部に記憶されている生体情報と同一の生体情報が生体情報読取手段から読み取られた場合に、前記送信手段から生体情報の送信を行わないようにする送信回避手段が設けられていることとしたものである。

【００５４】このため、一度読み取られた生体情報を読取生体情報記憶部に記憶させておき、この読取生体情報記憶部に記憶されている生体情報と同一の生体情報が読み取られた場合、送信回避手段によって生体情報の送信を拒否することができる。すなわち、他人が不正に特定人の生体情報を入手した場合、その生体情報を用いて生体情報の照合を行おうとしても、読取生体情報記憶部に記憶されている生体情報は用いることはできない。これは、例えば指紋のような生体情報では、押圧角度や押圧面積、或いは押圧力が同じである全く同一の生体情報が得られることはほとんどないことに基づくものである。このため、一度用いられた生体情報と全く同一の生体情報を再度用いることを防止することができる。

【００５５】さらに、他の発明は、上述の各発明に加えて更に、生体情報読取手段には、読み取られた生体情報が基準の品質以下の場合に再度生体情報の読み取りを行うようにする生体情報判別手段が設けられていることとしたものである。

【００５６】このため、生体情報により特定人か否かの照合を行う場合、基準の品質以上の生体情報にて特定人か否かの認証を行える。それによって、例えば生体情報読取手段の汚れによって一定基準以下の生体情報に基づく認証を行うのを防止することができ、認証精度の向上を図ることができる。

【００５７】また、他の発明は、ネットワークを介して特定人に係わる情報の管理を行い、その特定人に係わる情報にアクセスする者が特定人か否かを認証する認証方法において、生体情報を読み取る生体情報読取工程と、特定人の生体情報を照合用として登録している生体情報照合手段の生体情報と、生体情報読取工程によって読み取られた生体情報との照合を行う生体情報照合工程と、生体情報照合工程によって生体情報が符合した場合、この生体情報に対応するようにパスポート情報記憶手段に記憶されているパスポート情報を得るパスポート情報取得工程と、パスポート情報取得工程によって得られたパスポート情報に基づき、このパスポート情報に対応したサービスサイトにアクセスして該サービスサイトでのログオンを行うアクセス工程と、を具備することとしたものである。

【００５８】このため、生体情報を生体情報読取工程で読み取らせ、特定人の生体情報と符合すれば、パスポート情報記憶手段に記憶されているパスポート情報をパスポート情報取得工程で引き出して、アクセス工程によってこのパスポート情報に対応したサービスサイトにアクセスすることが可能となる。すなわち、生体情報の読み取りのみによって所定のサービスサイトにアクセス可能となり、複数のサービスサイトのＩＤやパスワードに対応させることができる。このため、一々複数のＩＤやパスワードを覚える必要がなく、利便性を向上させることが可能となる。すなわち、生体情報をシングルサイン感覚で読み取らせ、それに基づいた種々のサービスサイトの認証を行うことが可能となる。すなわち、ユーザは生体情報を自己の身分証明手段として用いるのみで、各サービスサイトでの認証を行うことが可能となる。

【００５９】さらに、他の発明は、上述の発明に加えて更に、生体情報照合工程での生体情報の照合に先立って、照合用として登録している特定人の生体情報を識別情報に基づいて検索する識別手段検索工程を具備していることとしたものである。

【００６０】このため、生体情報照合工程での照合に先立って、識別情報に基づいて登録されている生体情報を引き出すことが可能となる。すなわち、かかる識別情報に基づいて生体情報の検索を行うことによって、生体情報の照合を行う際の時間の短縮を図ることが可能となる。

【００６１】また、他の発明は、上述の各発明に加えて

更に、生体情報登録工程、生体情報照合工程、パスポート情報記憶工程及びアクセス工程はパスポートサーバ内で行われることとしたものである。

【００６２】このため、同一のパスポートサーバ内で、生体情報の照合や、それに対応したパスポート情報を引き出してアクセス工程によってサービスサイトにアクセスする。それによって、アクセス速度を速くすることが可能となる。

【００６３】さらに、他の発明は、上述の発明に加えて更に、生体情報読取工程は情報端末内で行われると共に、この生体情報読取工程によって読み取られた生体情報は、情報端末内で行われる送信工程によってパスポートサーバ内に伝送されることとしたものである。

【００６４】このため、情報端末単独で生体情報の読み取りを行い、この情報端末によって読み取られた生体情報を情報端末内の送信手段によって送信する。それにより、ユーザが所持可能な情報端末を用いて簡易に生体情報による認証を行い、この生体情報とパスポート情報との対応により、ユーザは生体情報をシングルサイン感覚で簡易に用いることが可能となる。

【００６５】また、他の発明は、上述の発明に加えて更に、生体情報読取工程で読み取られた生体情報に対して、生体情報照合工程に先立って、生体情報読取手段によって読み取られた生体情報のデータ処理を行うデータ処理工程と、データ処理工程によってデータ処理が為された生体情報から特徴点を抽出する特徴点抽出工程と、特徴点抽出工程によって特徴点が抽出された生体情報を、パスポートサーバの鍵情報記憶部に記憶されている独自の秘密鍵で暗号化するとともに、その後にパスポートサーバの鍵情報記憶部に記憶されている公開鍵で暗号化する暗号化工程と、を具備することとしたものである。

【００６６】このため、生体情報読取工程によって読み取られた生体情報に対して、まずデータ処理工程によってデータ処理を行う。続いて、データ処理工程でデータ処理が為された生体情報に対して、特徴点抽出工程で特徴点の抽出を行う。そして、特徴点が抽出された生体情報に対して、暗号化工程によって鍵情報記憶部に記憶されている独自の秘密鍵で暗号化した後に、パスポートサーバの公開鍵で暗号化を行う。このようにしてパスポートサーバに伝送すれば、例え伝送経路の途中で他人が不正に生体情報を入手しても、秘密鍵及び公開鍵で暗号化が為されているので、解読が極めて困難なものとなり、生体情報の伝送に際しての安全性を確保することができる。また、情報端末独自の秘密鍵で暗号化した後に、パスポートサーバ側の公開鍵で暗号化するので、伝送経路の途中で他人が不正に生体情報を入手し、入手した生体情報に基づいて改ざんを加えて他人が特定人に成りすまそうとしても、逆関数のないハッシュ関数の性質から、改ざんしたか否かを容易に検知することが可能となる。すなわち、事実上、特定人に成りすますことが不可能となる。

【００６７】さらに、他の発明は、上述の各発明に加えて更に、パスポート情報取得工程により得られるパスポート情報は、パスポート情報記憶手段内部においてアクセスレベルに分類されて記憶されていることとしたものである。

【００６８】このため、パスポート情報は、生体情報と対応するように設けられているので、生体情報読取工程において読み取られた生体情報に基づいて、この生体情報に対応したパスポート情報を引き出すことが可能となる。この場合、ＩＤやパスワードの如き単なる情報ではなく、生体情報を自己の身分証明手段として用いて認証を行うため、他人が特定人に成りすますのを防止することが可能となる。

【００６９】また、他の発明は、上述の発明に加えて更に、パスポート情報取得工程により得られるパスポート情報の前記パスポート情報記憶手段内部におけるアクセスレベルは、パスポート情報に関するデータの書込みや削除を行えるレベルと、パスポート情報に関するデータの存在を知ることができるレベルと、パスポート情報に関するデータの内容を見ることができるレベルと、パスポート情報に関するデータの書換えが行えるレベルと、パスポート情報に関するデータのワンタイムの書込みができるレベルと、パスポート情報に関するデータの利用ができるレベルに分類されていることとしたものである。

【００７０】このように各レベルに分けて分類したことにより、夫々のサービスサイトが要求する状態に、ユーザのアクセス権利を制限することが可能となる。これによって、生体情報の読み取りで該パスポート情報記憶手段にアクセスした場合、ユーザに対してもＩＤやパスワードの秘匿性を確保することも可能となる。

【００７１】さらに、他の発明は、上述の各発明に加えて更に、パスポート情報取得工程において、パスポート情報記憶手段にパスポート情報と共にこのパスポート情報に対応したＵＲＬも記憶されており、生体情報照合工程において生体情報が符合した場合に、パスポート情報記憶手段から対応するパスポート情報と共にサービスサイトのＵＲＬも引き出し、このＵＲＬに基づいてアクセス手段で該サービスサイトにアクセスすることとしたものである。

【００７２】このため、生体情報照合工程での照合で生体情報が符合した場合、パスポート情報記憶手段から対応するパスポート情報と共にサービスサイトのＵＲＬを引き出して、このＵＲＬに基づいてアクセス工程で特定のサービスサイトにアクセスすることが可能となる。すなわち、一々ＵＲＬを検索したり入力するせずに、特定のサービスサイトにアクセス可能となる。

【００７３】

19

【発明の実施の形態】以下、本発明の一実施の形態について、図１から図７に基づいて説明する。

【００７４】図６は、本発明の認証システム１０の概略を示すシステム図である。この図において、個人Ａは情報端末としてのクライアント端末１１を有している。クライアント端末１１には、例えばパーソナルコンピュータや、ＷＥＢ対応の携帯電話端末、或いは携帯情報端末（ＰＤＦ）がある。

【００７５】クライアント端末１１は、内部に生体情報読取手段１２を具備しており、この生体情報読取手段１２にて指紋等の生体情報の読み取りを行う構成である。ここで、生体情報読取手段１２により読み取られる生体情報には、指紋、虹彩、人のサイン、掌形、顔形、耳形、体臭、指の長さ、静脈の血管パターン、ＤＮＡ、声紋等がある。このうち、生体情報読取手段１２は、いずれかの生体情報を読み取れるように構成されている。代表的な生体情報読取手段１２としては、指紋認証スキャナや掌形認証スキャナ等がある。そして、クライアント端末１１には、かかる指紋認証スキャナ等の生体情報読取手段１２が内蔵されたり、或いはインターフェース１３を介して外部から取り付けられる。

【００７６】生体情報読取手段１２は、データ処理手段としてのＤＳＰ１４（Degital Signal Prosessor）やＣＰＵ１５（中央演算処理装置）等と接続されている。そして、生体情報読取手段１２の全ての行動は、ＣＰＵ１５によって監視される状態となる。

【００７７】指紋スキャナチップ等の生体情報読取手段１２は、ＤＳＰ１４に接続されている。ＤＳＰ１４は、生体情報読取手段１２によって読み取られたデジタルデータである生体情報の画像データ処理の演算を、高速で行うための回路である。この画像データ処理は、画像の細線化と２値化を行うものであり、例えば所定の太さを有する指紋を細くしたり、白黒のコントラスト８階調からなる画像データを、いずれかのしきい値で白と黒の２階調に分けるためのものである。

【００７８】そして、ＤＳＰ１４はＣＰＵ１５に接続されている。このＣＰＵ１５は、さらにメモリ領域１６とインターフェース１３を介して接続されている。メモリ領域１６は、ＲＡＭ１７とＲＯＭ１８を有している。このうち、ＲＡＭ１７は不揮発性メモリであり、データの読み込みや書きこみ、及びデータの書き換えを自由に行える、といった通常のＲＡＭが具備している性質を備えていると共に、電源を切っても記憶されているデータが消滅しない、といった性質を有しているメモリである。

【００７９】ここで、メモリ領域１６のＲＡＭ１７とＲＯＭ１８の内部構成として、以下の３パターンの構成が存在する。

【００８０】その１つ目は、図１に示すようなクライアント端末認証型の構成であり、クライアント端末１１内部で認証を行って、インターネットパスポートを取得するものである。このクライアント端末認証型のメモリ領域１６の構成は、ＲＡＭ１７に指紋特徴点データ等の生体情報特徴点データ２０が存在し、またこれと共にインターネットパスポート領域２１、及びワーク領域２２が存在する構成である。このうち、インターネットパスポート領域２１は、パスポート情報記憶手段としての役割を果たすものであり、電源を切っても消滅しないようになっている。

20

【００８１】また、ＲＯＭ１８には、オペレーションソフトウエア２３、特徴点抽出アルゴリズム２４、生体情報照合アルゴリズム２５、及び秘密鍵ＰＣ－Ｂ、公開鍵ＳＳ－Ａを記憶している鍵情報記憶部２６が格納されている。さらに、生体情報特徴点データ２０は、特定人の生体情報を照合用として登録しているものであり、生体情報登録手段としての機能を果たすものである。

【００８２】このうち、オペレーションソフトウエア２３は、情報端末が電源ＯＮとなったときに、最初にＣＰＵ１５に読み込まれるものである。このオペレーションソフトウエア２３には、上位アプリケーション、及び下位アプリケーションが存している。

【００８３】また、同じくＲＯＭ１８には、特徴点抽出手段としての特徴点抽出アルゴリズム２４が記憶されている。特徴点抽出アルゴリズム２４は、生体情報読取手段１２によって読み取られた生体情報から、特徴点の抽出を行うものである。そして、抽出された生体情報の特徴点は、照合用として予めＲＡＭ１７内に記憶されている。

【００８４】また、ＲＯＭ１８には、生体情報照合アルゴリズム２５が記憶されている。生体情報照合アルゴリズム２５は、生体情報読取手段１２によって読み取られ特徴点抽出アルゴリズム２４によって抽出された特徴点と、照合用の生体情報特徴点データ２０との照合を行う、生体情報照合手段としての機能を果たすものである。この生体情報照合アルゴリズム２５によって、生体情報読取手段１２で読み取られた生体情報が、特定人のものであるか否かの確認が行える構成である。

【００８５】なお、生体情報読取手段１２で読み取られ生体情報照合アルゴリズム２５で照合がなされた生体情報を記憶する読取生体情報記憶部を別途設け、さらにこの読取生体情報記憶部に記憶されている生体情報と同一の生体情報が生体情報読取手段から読み取られた場合に、生態情報照合アルゴリズム２５での照合を行わないようにする照合回避手段を設ける構成にしても構わない。

【００８６】また、ＲＯＭ１８には、鍵情報記憶部２６が設けられている。この鍵情報記憶部２６には、暗号化手段としての秘密鍵ＰＣ－Ｂ及び公開鍵ＳＳ－Ａが記憶されている。秘密鍵ＰＣ－Ｂは、クライアント端末１１が特有に有しているものであり、他には同一のものは存在しない。また、秘密鍵ＰＣ－Ｂは、サービスサイト４

０側に存する公開鍵ＰＣ－Ａと対を成す構成である。すなわち、秘密鍵ＰＣ－Ｂにより暗号化・復号化したデータは、サービスサイト４０側の公開鍵ＰＣ－Ａによって復号化・暗号化されるようになっている。さらに、公開鍵ＳＳ－Ａは、サービスサイト４０側の秘密鍵ＳＳ－Ｂと対を成す構成であり、サービスサイト４０側の秘密鍵ＳＶ－Ｂに対応した複数のものが存在する。公開鍵ＳＶ－Ａによって暗号化・復号化したデータは、サービスサイト４０側の秘密鍵ＳＶ－Ｂによってのみ復号化・暗号化されるようになっている。

【００８７】これら秘密鍵ＰＣ－Ｂ２６及び公開鍵ＳＳ－Ａは、ＲＯＭ１８内部に耐タンパー性を持たせて記憶されている。すなわち、ＲＯＭ１８は例えばワンチップのＬＳＩ内部に存するものであり、このワンチップ化されたＬＳＩ内部に秘密鍵ＰＣ－Ｂ２６と公開鍵ＳＳ－Ａが記憶され、それによって十分な耐タンパー性を持たせて構成されているものである。それ故、このＲＯＭ１８から秘密鍵ＰＣ－Ｂ及び公開鍵ＳＳ－Ａを読み取ることは、ほぼ不可能となっている。

【００８８】また、外部のパスポートサーバ５０等とデータの送信を行うため、クライアント端末１１には、送信手段２７が設けられている。

【００８９】なお、１つ目のタイプでは、サービスサイト４０側の数分だけ、対応する公開鍵ＳＳ－ＡがＲＯＭ１８内部に記憶されている。すなわち、ＲＯＭ１８には、秘密鍵ＰＣ－Ｂは、夫々のクライアント端末１１に特有なものが１つのみ記憶されていると共に、公開鍵ＳＳ－Ａは、ユーザが予め登録しているサービスサイト４０の分だけ記憶されている。

【００９０】また、１つ目のタイプのクライアント端末１１のワーク領域２２は、特徴点抽出アルゴリズム２４の起動、或いは生体情報照合アルゴリズム２５の起動のための作業領域であり、ＲＡＭ１７内部に一定の領域が確保されているものである。以上のようなＲＡＭ１７とＲＯＭ１８を備えたメモリ領域１６が、インターフェース１３に配置されて設けられている。

【００９１】また、図２に示す２つ目のタイプは、生体情報を照合して特定人であるか否かの認証は行うが、パスポート情報はパスポートサーバ５０側でないと得られない構成である。

【００９２】この２つ目のタイプのメモリ領域１６は、１つ目のタイプと異なってＲＡＭ１７内にインターネットパスポート領域２１が存在しない。代わりに、ＲＯＭ１８内にデポジットＩＤ３０及びデポジットＫｅｙ３１が記憶されている。それ故、生体情報読取手段１２で生体情報を読み取らせると、クライアント端末１１側で特定人であるか否かの認証を行い、特定人であると認証されたときに、デポジットＩＤ３０及びデポジットＫｅｙ３１を得る。それによって、パスポートサーバ５０側での認証を必要としない構成である。

【００９３】また、ＲＯＭ１８には、１つ目のタイプと同様に秘密鍵ＰＣ－Ｂが記憶されているが、１つ目のタイプとは異なって、サービスサイト４０側の公開鍵ＳＳ－Ａではなく、パスポートサーバ５０側の公開鍵ＳＶ－Ａが記憶されている。すなわち、２つ目のタイプでは、パスポートサーバ５０側の公開鍵ＳＶ－Ａを１つのみＲＯＭ１８に記憶している構成である。

【００９４】なお、その他の部分は、上述の１つ目のメモリ領域１６の構成と同様である。

【００９５】さらに、図３に示す３つ目のタイプのメモリ領域１６は、ＲＡＭ１７内にワーク領域２２が初期状態で存するのみである。また、ＲＯＭ１８内には、生体情報照合アルゴリズム２５が存せず、オペレーションソフトウエア２３、特徴点抽出アルゴリズム２４、秘密鍵ＰＣ－Ｂ、及び公開鍵ＳＶ－Ａが格納されているのみである。すなわち、この構成では、生体情報照合アルゴリズム２５がクライアント端末１１側には記憶されていない。その代わり、パスポートサーバ５０側にアクセスした状態で初めて生体情報の照合が行われる、いわばサーバ認証型の構成である。なお、ＲＡＭ１７に一度デポジットＩＤ３０を入力すれば、以後このデポジットＩＤ３０を記憶保存する、いわば識別情報記憶部を設けるように構成しても構わない。

【００９６】なお、以下の説明では、１つ目のタイプから３つ目のタイプの夫々で、パスポートサーバ５０側の構成が異なり、また作用も異なるため、夫々のタイプについて、説明することとする。また、以下の説明では、上述のクライアント端末１１側の作用をまず説明し、続いてパスポートサーバ５０側の構成の説明をすると共に、併せてパスポートサーバ５０側の作用についても説明する。

【００９７】（１つ目のタイプ）図１及び図４に示す１つ目のタイプのクライアント端末認証型のクライアント端末１１では、ユーザは、クライアント端末１１の電源をオンにする。すると、まず初めにＣＰＵ１５はオペレーションソフトウエア２３を読み込み、活動を開始する状態となる。しかしながら、生体情報読取手段１２の全ての行動は、インターフェース１３を介してオペレーションソフトウエア２３の上位アプリケーションの指示要求に基づいており、この生体情報読取手段１２自らが行動を行うことはない。すなわち、ＣＰＵ１５は、常時、インターフェース１３を監視している状態となる。

【００９８】この状態で、図４に示すようにユーザがクライアント端末１１を用いて特定のサービスサイト４０にアクセスする。そして、このサービスサイト４０でユーザが商品の購買を希望したり、情報コンテンツの閲覧やダウンロードを希望したとする。すると、このサービスサイト４０側では、ユーザの認証を行う必要があるため、ユーザに対して認証要求をする。この場合、例えばサービスサイト４０のＷｅｂ画面上に、「認証ボタン」

等を表示させ、この認証ボタンをクリックする。

【００９９】Ｗｅｂ画面上の認証ボタンをクリックした場合、クライアント端末１１は、認証実行状態となる。すなわち、ＣＰＵ１５は、例えばオペレーションソフトウエア２３に対して認証を実行させる状態となる。この状態で、ＣＰＵ１５が生体情報読取手段１２に対して「生体情報読取要求」を通知する。すると、ＣＰＵ１５は、ユーザに対し表示手段や音声を通じて生体情報読取手段１２によって生体情報を読み取らせるように指示を出す。なお、このような指示の表示を行うＬＥＤ、或いは音声を発するスピーカを別途設ける構成としても構わない。また、インターフェース１３を通じて、上位アプリケーションに対しても同様の指示を行う。すなわち、例えばパソコンの画面表示や音声等の如きマンマシンインターフェース１３を用いてユーザに生体情報の読み取り作業を行うよう、促すようにするものである。

【０１００】ここで、例えば指紋の如き生体情報の表面にごみや汚れがついている場合、或いは例えば指紋読取スキャナにおいて、スキャナチップの表面が汚れていて一定基準の品質の指紋画像が採取できない場合がある。この場合は、一定基準の品質をクリアする画像が採取できるまで、指紋画像の読み取りを行う。

【０１０１】続いて、ＣＰＵ１５は生体情報読取手段１２によって読み取られた生体情報を、ＲＡＭ１７のワーク領域２２に一時的に格納する。そして、ＣＰＵ１５は、ワーク領域２２に格納された生体情報をＤＳＰ１４に送り込み、画像処理を要求する。この場合の画像処理とは、細線化や２値化等である。細線化とは、指紋の模様を均一な細い線に変換する画像処理のことである。また、２値化とは、生画像が例えば８階調コントラストであるとき、この８階調コントラストをある一定値のコントラスト値、例えば４等をしきい値として、それ以下は黒、それ以上を黒としてコントラストを２階調に分けてしまうことである。

【０１０２】細線化や２値化等の画像処理が終了したら、ＤＳＰ１４は修理後画像をＲＡＭ１７のワーク領域２２に格納する。そして、ＣＰＵ１５に対して画像処理終了を通知する。この通知を受け取ったＣＰＵ１５は、特徴点抽出アルゴリズム２４を起動させ、処理後の画像をこの特徴点抽出アルゴリズム２４に手渡す。特徴点抽出アルゴリズム２４は、生体情報の画像の特徴点の抽出を行った後に、特徴点データをＲＡＭ１７のワーク領域２２に保存し、処理の終了をＣＰＵ１５に通知する。そして、特徴点抽出アルゴリズム２４は、自動的に処理を終了する。

【０１０３】なお、例えば生体情報として指紋データを用いた場合には、特徴点抽出方法は、例えば日本電気株式会社が採用しているマニューシャ抽出方式等を用いることが好ましい。しかしながら、かかるマニューシャ抽出方式以外にも、種々の方式を採用しても何等問題はない。

【０１０４】特徴点抽出アルゴリズム２４から処理終了通知を受け取ったＣＰＵ１５は、生体情報照合アルゴリズム２５を起動する。そして、ＣＰＵ１５は、生体情報照合アルゴリズム２５に対して、「生体情報照合要求」を行う。その後に、ＣＰＵ１５は、ＲＡＭ１７のワーク領域２２に存在する特徴点データを生体情報照合アルゴリズム２５に渡す。

【０１０５】ＣＰＵ１５から「生体情報照合要求」を受け取った生体情報照合アルゴリズム２５は、ワーク領域２２に存している特徴点データと、予めＲＡＭ１７に存している生体情報特徴点データ２０の照合処理を行う。その結果、ある一定のしきい値を下回っていれば、符合しなかったとしてその結果をＣＰＵ１５に通知する。また、ある一定のしきい値を上回っていれば、符合したとしてその結果をＣＰＵ１５に通知する。

【０１０６】ここで、生体情報が符合しなかった場合、ＣＰＵ１５は上位アプリケーションに対してインターフェース１３を介し、「認証できませんでした」等の表示を行い、ユーザに対して通知する。逆に、生体情報が符合した場合、ＣＰＵ１５はインターネットパスポート領域２１にアクセスする。そして、インターネットパスポート領域から、パスポート情報を取得可能となる。

【０１０７】なお、インターネットパスポート領域２１の詳細については、後述する（２つ目のタイプ）のインターネットパスポートデータベース５３の欄で説明する。通常、パスポート情報は、特定のサービスサイト４０へアクセスするためのＩＤやパスポート、或いはクレジットカード会社等の決済機関のカード番号やパスポート等である。以下、これらをパスポート情報として説明する。

【０１０８】この場合、取得されたパスポート情報は、「認証ボタン」がクリックされた特定のサービスサイト４０に、クライアント端末１１から伝送される。なお、特定のサービスサイト４０に対しては、特定のサービスサイト４０のパスポート情報に、後述するように暗号化を施してから伝送を行う方式でも良く、また特定のサービスサイト４０のパスポート情報に替えて、他の情報（例えば、認証ＯＫサイン等）に暗号化を施してから伝送を行う方式としても良い。なお、以下の説明では、特定のサービスサイト４０のパスポート情報に対して暗号化を施して伝送する場合について説明する。

【０１０９】クライアント端末１１から特定のサービスサイト４０のパスポート情報を該サービスサイト４０側に伝送する場合、このパスポート情報に対してオペレーションソフトウエア２３の有する暗号化処理機能によって暗号化処理が為される。すなわち、ＣＰＵ１５とオペレーションソフトウエア２３、及び秘密鍵ＰＣ－Ｂ、公開鍵ＳＳ－Ａによって暗号化手段が構成される。この暗号化処理では、特定のサービスサイト４０のパスポート

情報（ＩＤ及びパスワード等）を原文とすると共に、もう１つ同じパスポート情報のコピーを生成する。

【０１１０】そして、このコピーをハッシュ関数によって圧縮して原文のダイジェスト版を作成する。その後、送信者はダイジェスト版に対して自分の秘密鍵ＰＣ－Ｂで暗号化する。それにより、ダイジェスト版がデジタル署名となる。さらに、このデジタル署名を原文に添付する。そして、原文及び添付されたデジタル署名の両方に対し、サービスサイト４０側の公開鍵ＳＳ－Ａで暗号化し、送信対象を秘匿化する。そして、その後にＳＳＬ通信によってサービスサイト４０サーバ側に原文及びデジタル署名を暗号化データとして送信する。

【０１１１】ここで、ＳＳＬ（Secure Socket Layer）通信とは、Netscape Communications社が開発した、インターネット上で情報を暗号化して送受信するプロトコルを用いて行う通信方式である。ＳＳＬ通信では公開鍵暗号や秘密鍵暗号、デジタル証明書、ハッシュ関数などのセキュリティ技術を組み合わせ、データの盗聴や改ざん、なりすましを防ぐことができるように為されている。ＯＳＩ参照モデルではトランスポート層(第4層)にあたり、ＨＴＴＰやＦＴＰなどの上位のプロトコルを利用するアプリケーションからは、特に意識することなく透過的に利用することができる。

【０１１２】サービスサイト４０側で暗号化データを受信すると、まずサービスサイト４０側の鍵情報記憶部４１に記憶されている秘密鍵ＳＳ－Ｂによって復号化を行う。これは、公開鍵ＳＳ－Ａによって暗号化された暗号化データを復号化し得るのは、サービスサイト４０側が所持する秘密鍵ＳＳ－Ｂだからである。すると、サービスサイト４０側では、原文であるパスポート情報を得ると共に、デジタル署名を得ることになる。続いて、サービスサイト４０側では、同じく鍵情報記憶部４１に記憶されている公開鍵ＰＣ－Ａを用いてデジタル署名の検証を行う。そして、この検証によって、サービスサイト４０側では、原文のダイジェスト版を得ることができる。

【０１１３】すなわち、クライアント端末１１の秘密鍵ＰＣ－Ｂに対応した公開鍵ＰＣ－Ａを用いて検証することができれば、秘密鍵ＰＣ－Ｂを所持しているクライアント端末１１は、正当なクライアント端末１１である、とみなされる。それによって、クライアント端末１１の端末認証が、最初に為される。なお、このような検証は、サービスサイト４０側のサーバが有している復号化検証アルゴリズムによって為される。すなわち、ネットワークの途中で誰かが不正に暗号化データを入手し、これを改ざんした場合、改ざんされたデジタル署名によっては、ダイジェスト版が得られなく、それによって途中で改ざんされたか否かを検証することが可能となる。

【０１１４】上述の検証によって、正当なユーザであるとサービスサイト４０側で判断された場合には、復号化されたパスポート情報に基づいて、最終認証を行う。すなわち、パスポート情報がサービスサイト４０で利用できるものであるか否かの確認を行う。その結果、ユーザが該サービスサイト４０を利用できる者である、と判断された場合には、サービスサイト４０側では、ユーザに対して「ログオン承認」の通知を行う。以上のようにして、１つ目のタイプにおけるユーザの認証が為される。

【０１１５】（２つ目のタイプ）図２及び図５に示す２つ目のタイプのサーバ認証型のクライアント端末１１では、基本的に、ユーザが生体情報を読み取らせて、生体情報の照合を行う部分までは同じである。そして、この生体情報の照合を行ってから後の部分がやや異なるものとなっている。

【０１１６】生体情報が符合した場合、ＣＰＵ１５はＲＯＭ１８に格納されているデポジットＫｅｙ３１を、上述の１つ目のタイプで述べたような、自らの生体情報読取手段１２に対して発行されている公開鍵暗号インフラ方式を用いて暗号化する。なお、１つ目のタイプと異なって、２つ目のタイプではＲＯＭ１８にパスポートサーバ５０側の公開鍵ＳＶ－Ａが記憶されている。このため、デジタル署名及び原文は、公開鍵ＳＶ－Ａで暗号化されることとなる。

【０１１７】なお、２つ目のタイプでは、暗号化データと共に、サービスサイト４０のＵＲＬ情報も一緒に伝送する。このＵＲＬ情報は、暗号化されても暗号化されなくても構わない。

【０１１８】ＳＳＬ通信によってパスポートサーバ５０側に原文及びデジタル署名がクライアント端末１１から暗号化データとして送信され、パスポートサーバ５０側のアクセス手段５１でこの暗号化データを受信する。すると、上述の１つ目のタイプで述べたのと同じような暗号化データの復号化・検証が行われる。この場合、１つ目のタイプと異なって、復号化はパスポートサーバ５０の鍵情報記憶部５２に記憶されている秘密鍵ＳＶ－Ｂと公開鍵ＰＣ－Ａによって為される。また、この暗号化データの復号化・検証によって得られるのは、デポジットＩＤ３０及びデポジットＫｅｙ３１である。

【０１１９】なお、鍵情報記憶部５２には、後述する公開鍵ＳＳ－Ａも別途記憶されている。

【０１２０】パスポートサーバ５０側での復号化・検証により、正当なユーザであると判断された場合には、復号化されたデポジットＩＤ３０及びデポジットＫｅｙ３１に基づいて、パスポートサーバ５０が有しているインターネットパスポートデータベース５３の検索を行う。この検索は、インターネットパスポートデータベース５３に、復号化されたデポジットＩＤ３０及びデポジットＫｅｙ３１に対応するＷｅｂデポジット５４が存在するか否かの検索である。

【０１２１】なお、インターネットパスポートデータベース５３は、上述の１つ目のタイプにおけるインターネットパスポート領域２１が、各個人毎に複数存在して設

けられている。この場合、各個人毎のクライアント端末１１におけるインターネットパスポート領域２１は、Ｗｅｂを介したメモリ空間上に存在するので、各個人毎のＷｅｂデポジット５４となっている。そして、このＷｅｂデポジット５４がパスポート情報記憶手段としての機能を果たしている。

【０１２２】その結果、対応するＷｅｂデポジット５４が存在する場合には、このＷｅｂデポジット５４から対応するサービスサイト４０のパスポート情報を得る。この場合、Ｗｅｂデポジット５４から対応するサービスサイト４０のパスポート情報を得るために、ＵＲＬ情報に基づいてＷｅｂデポジット５４内の検索を行う。

【０１２３】ここで、パスポートサーバ５０に存するＷｅｂデポジット５４内のデータの構成について、例示で示した図７に基づいて説明する。この図に示すパスポート情報には、ユーザのアクセス権利によって、以下のレベルに分類されている。この図に示すように、ユーザのアクセス権利の分類は、＜書込み許可権利・削除権利＞、＜存在を知ることができる＞、＜内容を見ることができる＞、＜書換えできる＞、＜ワンタイム書込みができる＞、＜利用できる＞となっている。

【０１２４】また、ユーザのパスポート情報には、例えば、「デポジットＩＤ」、「第三者機関記載情報」、「サービスサイト記載情報」、「公的機関記載情報」、「民間企業記載情報」、「ユーザ記載情報」、「生体情報」、「アルゴリズム」がある。

【０１２５】これらのパスポート情報のアクセスレベルは、例えばフラグの設定によって行う。すなわち、例えばデポジットＩＤ３０専用のフォルダを作成し、このフォルダのプロパティ中のフラグの設定を行うことにより為される。例示したデポジットＩＤ３０へのアクセス権利では、＜書込み許可権利・削除権利＞という権利はないので、これに対応したフラグを「０」に設定する。また、＜存在を知ることができる＞という権利はあるので、これに対応したフラグを「１」に設定する。

【０１２６】また、別のアクセスレベルの分類としては、全てのアクセス権利を有する、フルアクセス可能な状態を数字の「０」で表し、以下、アクセス権利が制限されるに従って、大きな数字を割り振ることにより行うものがある。この場合では、＜書込み許可権利・削除権利＞～＜利用できる＞までの行と、「デポジットＩＤ」～「アルゴリズム」までの列における組み合わせの分だけ数字を割り振り、その数字にアクセス権利を対応させる。このようにしても、アクセス権利の制御が実現可能となる。

【０１２７】なお、「決済機関情報」や、「サービスサイト情報」等は、複数の決済機関情報や複数のサービスサイト情報が記載されているため、複数の情報を保存しておくフォルダを形成し、このフォルダ毎にフラグの設定を行うように構成しても構わない。

【０１２８】以上の如く、ユーザのアクセス権利の分類がなされたものの例示としては、「○」ができる、「×」ができない、「△」がサービスサイト４０の方針でできたりできなかったりする、で示す。この場合、「デポジットＩＤ」は、＜書込み許可権利・削除権利＞は×、＜存在を知ることができる＞は○、＜内容を見ることができる＞は○、＜書換えできる＞は×、＜ワンタイム書込みができる＞は×、＜利用できる＞は○となっている。また、「第三者機関記載情報」、「決済機関情報」、「サービスサイト記載情報」、「公的機関記載情報」、及び「民間企業記載情報」は、＜書込み許可権利・削除権利＞は○、＜存在を知ることができる＞は○、＜内容を見ることができる＞は△、＜書換えできる＞は×、＜ワンタイム書込みができる＞は×、＜利用できる＞は○となっている。

【０１２９】さらに、「ユーザ記載情報」は、＜書込み許可権利・削除権利＞は○、＜存在を知ることができる＞は○、＜内容を見ることができる＞は○、＜書換えできる＞は○、＜ワンタイム書込みができる＞は×、＜利用できる＞は○となっている。また、「生体情報」は、＜書込み許可権利・削除権利＞は×、＜存在を知ることができる＞は○、＜内容を見ることができる＞は×、＜書換えできる＞は×、＜ワンタイム書込みができる＞は○、＜利用できる＞は○となっている。また、「アルゴリズム」は、＜書込み許可権利・削除権利＞は×、＜存在を知ることができる＞は○、＜内容を見ることができる＞は×、＜書換えできる＞は×、＜ワンタイム書込みができる＞は×、＜利用できる＞は○となっている。

【０１３０】しかしながら、アクセス権利の設定は、上述のものには限られず、インターネットパスポートデータベース５３の管理者は、パスポート情報の重要性に鑑みて種々設定可能である。

【０１３１】このような構成のデポジット領域から、必要なパスポート情報がパスポートサーバ５０に引き出されると、このパスポート情報に基づいて、パスポートサーバ５０はアクセス手段５１を介してログオン要求が為されている特定のサービスサイト４０のサーバにアクセスする。なお、特定のサービスサイト４０へのログオンは、パスポート情報と共に伝送されてきたＵＲＬに基づいて行う。

【０１３２】この場合、パスポート情報がパスポートサーバ５０に引き出されると、このパスポート情報に基づいて、特定のサービスサイト４０にログオン要求が為される。この場合、特定のサービスサイト４０に対してパスポート情報を伝送することになるが、該特定のサービスサイト４０へのパスポート情報の伝送に際しては、パスポート情報に対して暗号化を施して伝送する。

【０１３３】すなわち、上述の１つ目のタイプで説明したクライアント端末１１での暗号化手段による暗号化処理と同様に、パスポート情報を原文とすると共に、もう

１つの同じパスポート情報のコピーを生成する。そして、このコピーをハッシュ関数によって圧縮して原文のダイジェスト版を作成する。その後、送信者はダイジェスト版に対してパスポートサーバ５０側の秘密鍵ＳＶ－Ｂで暗号化する。それにより、ダイジェスト版がデジタル署名となる。さらに、このデジタル署名を原文に添付する。そして、原文及び添付されたデジタル署名に対し、サービスサイト４０側の公開鍵ＳＳ－Ａで、原文とそれに添付したデジタル署名の両方を暗号化し、送信対象を秘匿化する。そして、その後にＳＳＬ通信によってサービスサイト４０側に原文及びデジタル署名を暗号化データとして送信する。

【０１３４】サービスサイト４０側で暗号化データを受信すると、まずサービスサイト４０側の鍵情報記憶部４１に存している秘密鍵ＳＳ－Ｂによって復号化を行う。これは、公開鍵ＳＳ－Ａによって暗号化された暗号化データを復号化し得るのは、パスポートサーバ５０が所持する秘密鍵ＳＳ－Ｂだからである。すると、パスポートサーバ５０側では、原文であるパスポート情報を得ると共に、デジタル署名を得ることになる。続いて、サービスサイト４０側では、鍵情報記憶部４１に存している公開鍵ＳＶ－Ａを用いてデジタル署名の検証を行う。そして、この検証によって、パスポートサーバ５０側では、原文のダイジェスト版を得ることができる。

【０１３５】このように、パスポートサーバ５０の秘密鍵ＳＶ－Ｂに対応した公開鍵ＳＶ－Ａを用いて検証することができれば、秘密鍵ＳＶ－Ｂを所持しているパスポートサーバ５０は、正当なものである、とみなされる。それによって、パスポートサーバ５０の端末認証が、最初に為される。なお、このような検証は、パスポートサーバ５０が有している復号化検証アルゴリズムによって為される。すなわち、ネットワークの途中で誰かが不正に暗号化データを入手し、これを改ざんした場合、改ざんされたデジタル署名によっては、ダイジェスト版が得られなく、それによって途中で改ざんされたか否かを検証することが可能となる。

【０１３６】上述の検証によって、パスポートサーバ５０が正当なものであるとサービスサイト４０側で判断された場合には、復号化されたパスポート情報に基づいて、最終認証を行う。すなわち、パスポート情報がサービスサイト４０で利用できるものであるか否かの確認を行う。その結果、ユーザが該サービスサイト４０を利用できる者である、と判断された場合には、サービスサイト４０側では、ユーザに対して「ログオン承認」の通知を行う。以上のようにして、２つ目のタイプにおけるユーザの認証が為される。

【０１３７】（３つ目のタイプ）３つ目のタイプのサーバ認証型では、クライアント端末１１側で生体情報の照合を行わないものである。この３つ目のタイプでは、１つ目のパターン及び２つ目のパターンで述べた特徴点抽出アルゴリズム２４によって生体情報の特徴点抽出を行う部分までは、同じである。そして、ここから後の部分がやや異なるものとなっている。

【０１３８】特徴点抽出アルゴリズム２４によって生体情報の特徴点を抽出し、この終了通知をＣＰＵ１５が受け取った後に、ＲＡＭ１７のワーク領域２２に存在する特徴点データを自らのクライアント端末１１（生体情報読取手段１２）に対して発行されている秘密鍵ＰＣ－Ｂで暗号化する。この場合、特徴点データのみならず、クライアント端末１１がデポジットＩＤ３０を記憶している場合には、このデポジットＩＤ３０も一緒に秘密鍵ＰＣ－Ｂで暗号化する。

【０１３９】なお、以下の暗号化の手順は、上述の２つ目のタイプで述べたデポジットＩＤ３０及びデポジットＫｅｙ３１の暗号化の手順と同じである。すなわち、原文を特徴点が抽出された生体情報（特徴点データ）及びデポジットＩＤ３０とし、この原文に対してコピーを作成する。そして、このコピーをハッシュ関数によって圧縮して原文のダイジェスト版を作成する。その後に、このダイジェスト版をクライアント端末１１側の秘密鍵ＰＣ－Ｂで暗号化してデジタル署名を作成する。

【０１４０】そして、このデジタル署名を原文に添付し、原文及び添付されたデジタル署名の両方をパスポートサーバ５０側の公開鍵ＳＶ－Ａで暗号化して全体の秘匿化を図る。そして、この後にＳＳＬ通信によってパスポートサーバ５０側に原文及びデジタル署名を暗号化データとして送信する。

【０１４１】なお、３つ目のタイプでも、暗号化データと共にサービスサイト４０のＵＲＬ情報も一緒に伝送する。このＵＲＬ情報は、暗号化されても暗号化されなくても構わない。

【０１４２】パスポートサーバ５０側のアクセス手段５１で暗号化データを受信すると、まずパスポートサーバ５０側の鍵情報記憶部５２に存している秘密鍵ＳＶ－Ｂで復号化を行う。すると、パスポートサーバ５０側では、原文である生体情報（特徴点データ）及びデポジットＩＤを得ると共に、デジタル署名を得ることとなる。続いて、パスポートサーバ５０側では、鍵情報記憶部５２の公開鍵ＰＣ－Ａを用いてデジタル署名の検証を行う。そして、この検証によって、パスポートサーバ５０側では、原文のダイジェスト版を得ることができる。このダイジェスト版が得られるか否かで、デジタル署名が改ざんされたか否かを検証することができる。

【０１４３】ここで、パスポートサーバ５０内には、照合用の生体情報が生体情報データベース５５に登録されている。この生体情報データベース５５は、上述の１つ目のタイプ及び２つ目のタイプにおける生体情報特徴点データ２０に対応するものである。かかる生体情報データベース５５は、各個人毎の生体情報特徴点データ２０を、多人数分登録しているものである。

【０１４４】また、生体情報データベース５５には、生体情報照合手段５６が接続されている。生体情報照合手段５６は、上述の１つ目のタイプ及び１つ目のタイプにおけるのと同様な生体情報照合アルゴリズム５７を有するものである。なお、３つ目のタイプにおいては、かかる生体情報アルゴリズム５７と共に、生体情報データベース５５から引き出された照合用の生体情報特徴点データ２０を引き出して作業するためのメモリ空間５８も有する構成である。

【０１４５】生体情報での認証を行う場合には、復号された生体情報（特徴点データ）と、生体情報データベース５５から照合用の生体情報特徴点データ２０とを生体情報照合手段５６のメモリ空間５８に引き出す。そして、生体情報照合アルゴリズム５７にてこれら両生体情報の照合を行う。

【０１４６】この照合の結果、両生体情報が符合すると判断された場合、生体情報照合手段５６から「ＯＫ」のサインがアクセス手段５１に出される。このアクセス手段５１が「ＯＫ」のサインを受け取った場合、アクセス手段５１からインターネットパスポートデータベース５３にパスポート表示命令が出される。なお、インターネットパスポートデータベース５３の構成は、上述の１つ目のパターンで述べたのと同様である。

【０１４７】また、インターネットパスポートデータベース５３からアクセス手段５１にパスポート情報が引き出され、特定のサービスサイト４０にログオン要求する場合も、上述の２つ目のタイプと同様である。

【０１４８】このように、３つ目のタイプは、生体情報を２つ目のタイプにおけるデポジットＫｅｙ３１に見立て、デポジットＩＤ３０及びデポジットＫｅｙ３０に対応するＷｅｂデポジット５４を検索し、このＷｅｂデポジット５４から目的とするパスポート情報を得るものである。

【０１４９】なお、３つ目のタイプでは、生体情報データベース５４と生体情報照合手段５６を、パスポートサーバ５０から分離して、別途認証サーバに設ける構成としても構わない。パスポートサーバ５０と別途の認証サーバを設ける場合には、これらパスポートサーバ５０と認証サーバの間がネットワーク回線によって接続されている。

【０１５０】このような構成の認証システム１０、認証方法によると、１つ目のタイプから３つ目のタイプまで、共に生体情報を生体情報読取手段１２で読み取り、特定人の生体情報と符合させる。そして、生体情報が符合すれば、Ｗｅｂデポジット５４に記憶されているパスポート情報を引き出して、パスポートアクセス手段によってこのパスポート情報に対応したサービスサイト４０にアクセスする。このため、生体情報の読み取りのみによって所定のサービスサイト４０にアクセス可能となり、複数のサービスサイト４０のＩＤやパスワードに対応させることができる。

【０１５１】このようにしたことで、一々複数のＩＤやパスワードを覚える必要がなく、利便性を向上させることが可能となる。すなわち、生体情報をシングルサイン感覚で読み取らせ、それに基づいた種々のサービスサイト４０の認証を行うことが可能となる。また、ユーザは生体情報を自己の身分証明手段として用いるのみで、各サービスサイト４０での認証を行うことが可能となる。

【０１５２】また、読取生体情報記憶部と照合回避手段を設けた場合には、一度読み取られた生体情報を読取生体情報記憶部に記憶させておき、この読取生体情報記憶部に記憶されている生体情報と同一の生体情報に基づく照合を、照合回避手段で拒否することができる。すなわち、他人が不正に特定人の生体情報を入手した場合、その生体情報を用いて生体情報の照合を行おうとしても、読取生体情報記憶部に記憶されている生体情報を用いることはできない。これは、例えば指紋のような生体情報では、押圧角度や押圧面積、或いは押圧力が同じである全く同一の生体情報が得られることはほとんどないことに基づくものである。

【０１５３】このような読取生体情報記憶部、及び照合回避手段をパスポートサーバ５０内に設けた場合には、パスポートサーバ５０内に一度照合した生体情報を蓄えておくことができる。そして、蓄えられた生体情報と同一の生体情報がパスポートサーバ５０に送信されてきた場合には、照合回避手段で生体情報の照合を回避することが可能となる。すなわち、２つ目のタイプ及び３つ目のタイプに適したものとなる。

【０１５４】また、読取生体情報記憶部、及び照合回避手段をクライアント端末１１内に設けた場合には、クライアント端末１１側で一度照合した生体情報を蓄えて奥ことができ、この蓄えられた生体情報と同一の生体情報が生体情報読取手段１２で読み取られた場合には、照合回避手段で生体情報の照合を回避することが可能となる。

【０１５５】また、１つ目のタイプでは、クライアント端末１１に生体情報特徴点データと、生体情報照合アルゴリズム２５と、インターネットパスポート領域２１と、を有している。そのため、クライアント端末１１側で特定人か否かの認証が行え、この認証に基づいてインターネットパスポート領域２１からパスポート情報を取得し、このパスポート情報に基づいて特定のサービスサイト４０にアクセス可能となる。

【０１５６】また、２つ目のタイプでは、クライアント端末１１に生体情報特徴点データと、生体情報照合アルゴリズム２５と、を有している。このようにすることで、クライアント端末１１側で特定人か否かの認証が行え、この認証に基づいてデポジットＫｅｙ３１を取得し、デポジットＩＤ３０及びデポジットＫｅｙ３１に基づいてインターネットを介してインターネットパスポー

トデータベース５３にアクセスすることができる。

【０１５７】また、３つ目のタイプでは、クライアント端末１１で特定人か否かの認証は行わずに、パスポートサーバ５０側で特定人か否かの認証を行い、この認証に基づいてインターネットパスポートデータベース５３にアクセスするものである。このようにすることで、完全にパスポートサーバ５０側で認証を行う構成となる。すなわち、１つ目のタイプ及び２つ目のタイプと異なって、３つ目のタイプでは、クライアント端末１１を交換しても、特定人か否かの認証を行うことが可能となる。

【０１５８】また、３つ目のタイプにおいては、生体情報照合手段とインターネットパスポートデータベース５３とが同一のパスポートサーバ５０内に設けられている。このため、生体情報を照合してインターネットパスポートデータベース５３からパスポート情報を引き出す場合、パスポート情報の引き出しまでの時間の短縮化を図ることが可能となる。

【０１５９】また、３つ目のタイプでは、クライアント端末１１単独で生体情報の読み取りを行い、読み取られた生体情報をパスポートサーバ５０に伝送するものである。このため、ユーザが所持可能なクライアント端末１１を用いて簡易に生体情報を読み取らせ、読み取らせた生体情報とパスポート情報を対応させることで、生体情報をサービスサイト４０に対する身分証明手段として、シングルサイン感覚で簡易に用いることが可能となる。

【０１６０】また、クライアント端末１１は、ＤＳＰ１４、特徴点抽出アルゴリズム２４、鍵情報記憶部２６及び暗号化手段としてのオペレーションソフトウエア２３、秘密鍵ＰＣ－Ｂ、公開鍵ＳＶ－Ａ（公開鍵ＳＳ－Ａ）を有している。このため、ＤＳＰ１４でデータ処理が為され、特徴点抽出アルゴリズム２４で特徴点の抽出が為された生体情報に対して秘密鍵ＰＣ－Ｂで暗号化した後に公開鍵ＳＶ－Ａ（公開鍵ＳＳ－Ａ）で暗号化を行う。このようにしてからパスポートサーバ５０に伝送すれば、例え伝送経路の途中で他人が不正に生体情報を入手しても、解読が極めて困難なものとなり、生体情報の伝送に際しての安全性を確保することが可能となる。

【０１６１】また、クライアント端末１１独自の秘密鍵ＰＣ－Ｂで暗号化した後に、パスポートサーバ５０側の公開鍵ＳＶ－Ａ（公開鍵ＳＳ－Ａ）で暗号化するので、伝送経路の途中で他人が不正に生体情報を入手し、入手した生体情報に基づいて改ざんを加えて他人が特定人に成りすまそうとしても、逆関数のないハッシュ関数の性質から、改ざんしたか否かを容易に検知することが可能となる。すなわち、事実上、特定人に成りすますことが不可能となる。

【０１６２】さらに、２つ目のタイプ及び３つ目のタイプでは、生体情報が生体情報データベース５４に登録されるに際してデポジットＩＤ３０が割り当てられている。このため、生体情報照合手段５６での生体情報の照合を行うに先立って、このデポジットＩＤ３０に基づいて生体情報データベース５４に登録されている生体情報特徴点データ２０を特定することが可能となる。すなわち、かかるデポジットＩＤ３０に基づいて生体情報の検索を行うことにより、生体情報の照合の時間の短縮化を図ることができる。

【０１６３】また、かかるデポジットＩＤ３０をクライアント端末１１に記憶させることにより、クライアント端末１１側で生体情報の読み取りを行って伝送する場合、一々特定人がデポジットＩＤ３０を入力しなくても済む。なお、このデポジットＩＤ３０も暗号化すれば、デポジットＩＤ３０の秘匿化を図ることができ、このデポジットＩＤ３０の解読が極めて困難となって安全性を確保することができる。

【０１６４】さらに、Ｗｅｂデポジット５４は、アクセスレベル別に分類されている。ここで、パスポート情報は、生体情報と対応するように設けられているので、生体情報読取手段１２によって生体情報を読み取らせると、この生体情報に対応したパスポート情報を引き出すことができる。この場合、ＩＤやパスワードの如き単なる情報ではなく、生体情報を自己の身分証明手段として用いて認証を行うため、他人が特定人に成りすますのを防止することができる。

【０１６５】さらにユーザのアクセスレベルの設定により、ネットを介しての会員制サービスサイト、或いは決済機関、公的機関、民間企業等が運営する、種々のサービスサイトにメリットが生ずることとなる。例えば、決済機関の情報を記載している場合、ユーザのアクセスレベルを「存在を知ることができる」を○として、「書換えできる」を×とした場合、ユーザは勝手にパスポート情報であるＩＤやパスワードを書き換えることができない。このようなアクセスレベルの設定により、各サイト側において生体情報を活用した本人の絶対認証を現実的に利用可能となる。

【０１６６】また、例えばデータを保存する領域をＷｅｂデポジット５４内に設けた場合、アクセスレベルの設定の仕方によってはデータの保存はできるがコピーはできないようにすることもできる。この場合には、特定人は生体情報を用いてアクセス可能となり、Ｗｅｂデポジット５４内でそのデータをアクセスレベルに設定されたレベル内で利用可能となるが、違法なコピー等は行えないものとなる。それによって、種々のコンテンツからデータを該Ｗｅｂデポジット５４内にダウンロードした場合、他の領域にはコピーできないため、該データの著作権を守ることが可能となる。

【０１６７】また、Ｗｅｂデポジット５４のアクセスレベルは、パスポート情報に関するデータの書込みや削除を行えるレベルと、パスポート情報に関するデータの存在を知ることができるレベルと、パスポート情報に関するデータの内容を見ることができるレベルと、パスポー

ト情報に関するデータの書換えが行えるレベルと、パスポート情報に関するデータのワンタイムの書込みができるレベルと、パスポート情報に関するデータの利用ができるレベルに分類されている。

【０１６８】このように各レベルに分けて分類したことにより、夫々のサービスサイト４０が要求する状態に、ユーザのアクセス権利を制限することが可能となる。これによって、生体情報の読み取りで該Ｗｅｂデポジット５４にアクセスした場合、ユーザに対してもＩＤやパスワードの秘匿性を確保することも可能となる。

【０１６９】さらに、アクセスレベルの設定は、フラグの設定によってアクセスレベルを種々設定するので、簡易な操作でサービスサイト側の希望に沿ったアクセスレベルにＷｅｂデポジット５４を設定できる。

【０１７０】なお、アクセスレベルの設定は、アクセスレベル別に割り当てられた数字の設定によって行うこともできる。このようにアクセスレベル別に割り当てられた数字の設定によってアクセスレベルを種々設定する場合も、簡易な操作でサービスサイト側の希望に沿ったアクセスレベルにＷｅｂデポジット５４を設定することができる。

【０１７１】また、Ｗｅｂデポジット５４には、パスポート情報に対応したサービスサイト４０のＵＲＬも記憶されておくこともできる。この場合、生体情報データベース５５に登録された生体情報と、生体情報読取手段１２によって読み取られた生体情報とが符合した場合に、Ｗｅｂデポジット５４から対応するパスポート情報と共にサービスサイト４０のＵＲＬを引き出して、このＵＲＬに基づいてアクセス手段５１で特定のサービスサイト４０にアクセスすることが可能となる。すなわち、一々ＵＲＬを検索したり入力せずに、特定のサービスサイト４０にアクセス可能となる。

【０１７２】さらに、生体情報読取手段１２には、読み取られた生体情報が基準の品質以下の場合に再度生体情報の読み取りを行うようにする生体情報判別手段を設けるようにしても良い。このように構成した場合には、基準の品質以上の生体情報にて特定人か否かの認証を行える。それによって、例えば生体情報読取手段の汚れによって一定基準以下の生体情報に基づく認証を行うのを防止することができ、認証精度の向上を図ることができる。

【０１７３】以上、本発明の一実施の形態について説明したが、本発明はこれ以外にも種々変形可能である。以下、それについて説明する。上述の実施の形態では、デジタル署名を秘密鍵ＰＣ－Ｂで暗号化し、このデジタル署名と原文とを公開鍵ＳＳ－Ａ（ＳＶ－Ａ）で暗号化してからＳＳＬ通信で送信している。しかしながら、デジタル署名を生成せずに、単に原文を秘密鍵ＰＣ－Ｂで暗号化した後に、公開鍵ＳＳ－Ａ（ＳＶ－Ａ）で暗号化してからＳＳＬ通信で送信するように構成しても構わない。

【０１７４】また、図６では、生体情報特徴点データ２０は、Ｗｅｂデポジット５４とは別個に設けられた生体情報データベース５５に登録されているが、生体情報特徴点データ２０を各個人毎のＷｅｂデポジット５４内に登録させる構成としても構わない。このように、生体情報特徴点データ２０をＷｅｂデポジット５４内に登録する構成とした場合は、Ｗｅｂデポジット５４の構成を示す図７の「生体情報」の欄に登録することとなる。

【０１７５】また、Ｗｅｂデポジット５４に「生体情報」の欄を設けた場合、生体情報照合手段５６をインターネットデータベース５３内に設けるようにしても良い。この場合、インターネットデータベース５３は、サーバ的な機能を果たすことになり、インターネットデータベース５３とアクセス手段５１との間で直接やり取りする構成となる。

【０１７６】また、「生体情報」をＷｅｂデポジット５４内に設けると共に、生体情報アルゴリズム５７を各個人毎のＷｅｂデポジット５４内に設ける構成としても構わない。この場合、生体情報の照合は、全てＷｅｂデポジット５４内で行える構成となり、セキュリティが向上する構成となる。この構成を採用する場合、Ｗｅｂデポジット５４内の「アルゴリズム」の欄に生体情報アルゴリズムを記憶させておく。

【０１７７】

【発明の効果】本発明によれば、生体情報を生体情報読取手段で読み取り、特定人の生体情報と符合すれば、パスポート情報記憶手段に記憶されているパスポート情報を引き出して、アクセス手段によってこのパスポート情報に対応したサービスサイトにアクセスすることが可能となる。すなわち、生体情報の読み取りのみによって所定のサービスサイトにアクセス可能となり、複数のサービスサイトのＩＤやパスワードに対応させることができる。このため、一々複数のＩＤやパスワードを覚える必要がなく、利便性を向上させることが可能となる。すなわち、生体情報をシングルサイン感覚で読み取らせ、それに基づいた種々のサービスサイトの認証を行うことが可能となる。すなわち、ユーザは生体情報を自己の身分証明手段として用いるのみで、各サービスサイトでの認証を行うことが可能となる。

【図面の簡単な説明】

【図１】本発明の認証システムにおけるクライアント端末のうち、１つ目のタイプの構成を示す図である。

【図２】本発明の認証システムにおけるクライアント端末のうち、２つ目のタイプの構成を示す図である。

【図３】本発明の認証システムにおけるクライアント端末のうち、３つ目のタイプの構成を示す図である。

【図４】図１のクライアント端末を用いた認証システムの構成を示す図である。

【図５】図２のクライアント端末を用いた認証システム

の構成を示す図である。

【図６】図３のクライアント端末を用いた認証システムの構成を示す図である。

【図７】図１のクライアント端末のインターネットパスポート領域、又は図２若しくは図３の認証システムにおけるＷｅｂデポジットの構成を示す図である。

【図８】従来のリアル世界、準バーチャル世界、及びバーチャル世界における認証の差異を示す図である。

【符号の説明】

１０…認証システム

１１…クライアント端末（情報端末）

１２…生体情報読取手段

１４…ＤＳＰ（データ処理手段）

１５…ＣＰＵ

１７…ＲＡＭ

１８…ＲＯＭ

２０…生体情報特徴点データ（生体情報登録手段）

２１…インターネットパスポート領域（パスポート情報記憶手段）

２３…オペレーションソフトウエア

２４…特徴点抽出アルゴリズム

２５…生体情報照合アルゴリズム（生体情報照合手段）

２６…鍵情報記憶部

２７，４１，５２…送信手段

３０…デポジットＩＤ

３１…デポジットＫｅｙ

４０…サービスサイト

５０…パスポートサーバ

５１…アクセス手段

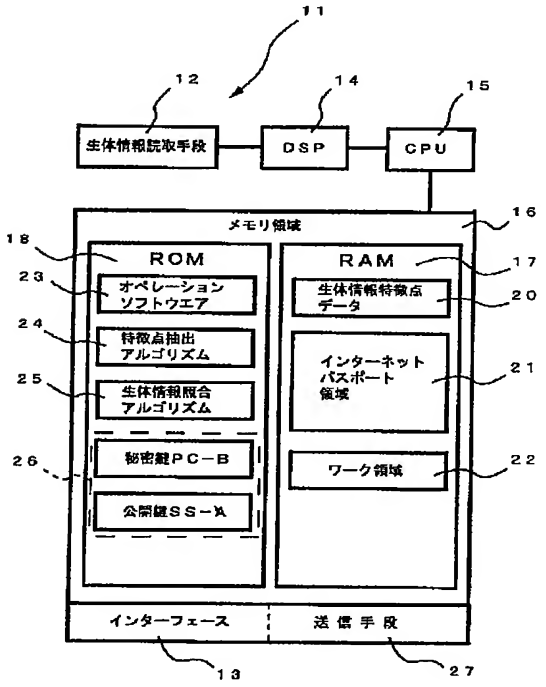
５３…インターネットパスポートデータベース

５４…Ｗｅｂデポジット

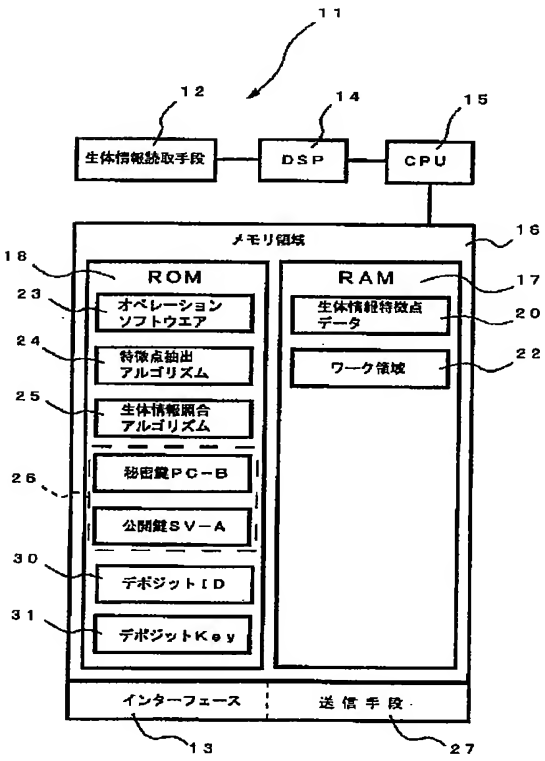
５５…生体情報データベース（生体情報登録手段）

５６…生体情報照合手段

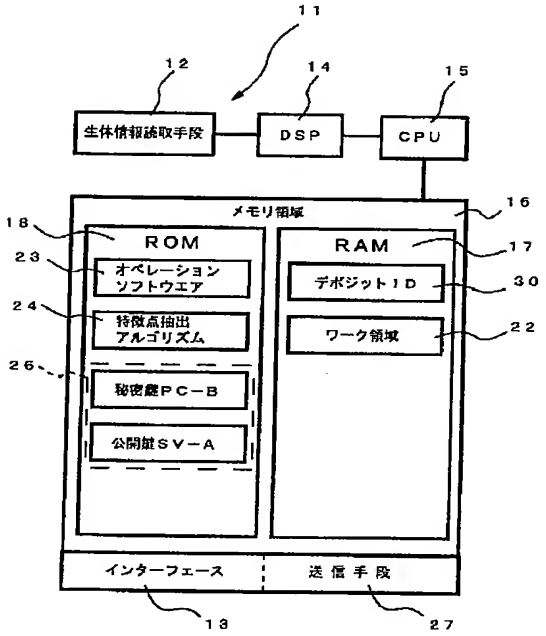
【図１】



【図２】



【図３】



【図７】

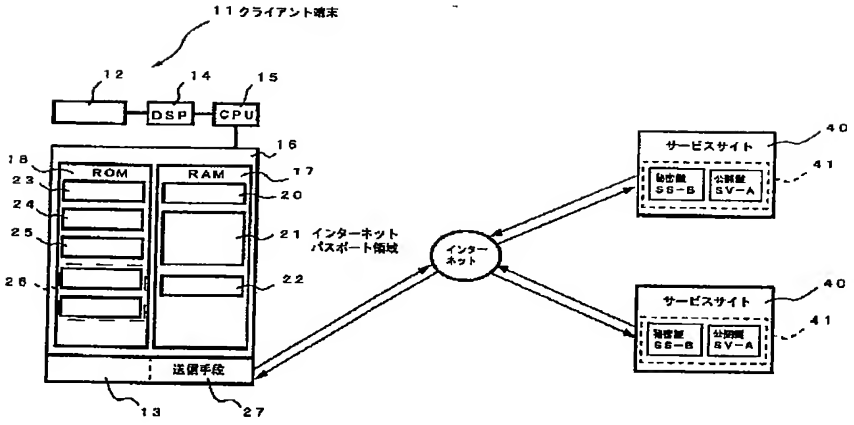
Ｗｅｂデポジット５４の構成

ユーザーのアクセス権利

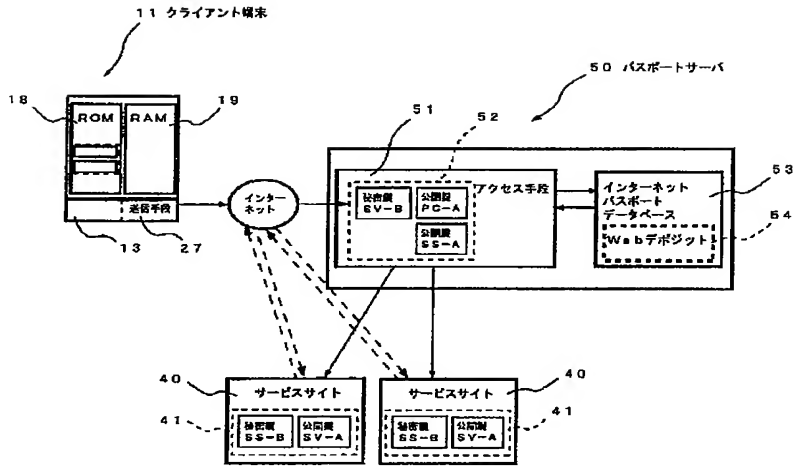
	書込み許可権利・削除権利	存在を知ることができる	内容を見ることができる	書換えできる	ワンタイム書込みができる	利用出来る
Deposit ID	×	○	○	×	×	○
第三者機関記載情報	○	○	△	×	×	○
決済機関記載情報	○	○	△	×	×	○
サービスサイト記載情報	○	○	△	×	×	○
公的機関記載情報	○	○	△	×	×	○
民間企業記載情報	○	○	△	×	×	○
ユーザー記載情報	○	○	○	○	×	○
生体情報	×	○	×	×	○	○
アルゴリズム	×	○	×	×	×	○

○:出来る　×:出来ない　△:サービスサイトの方針で出来たり出来なかったりする。

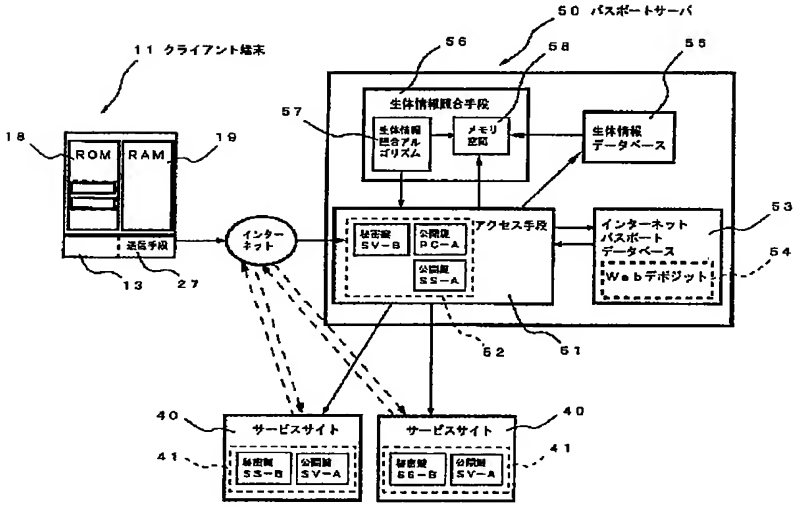
【図４】



【図５】



【図６】



【図８】

	リアル世界	半バーチャル世界	バーチャル世界
ハードウェアトークンの所有認証	○	○	×
ハードウェアトークンが偽造されていないか？	△	△	×
記憶トークンの記憶認証	○	○	○
記憶トークンが盗まれていないか？	×	×	×
顔認証	○	×	×
虹彩認証	○	×	×
監視カメラ撮影（防犯・バックアップ）	○	○	×

フロントページの続き

(51)Int.Cl.[7]		識別記号	FI		テーマコード(参考)
Ｇ０９Ｃ	1/00	６４０	Ｇ０９Ｃ	1/00	６４０Ｂ
Ｈ０４Ｌ	9/32		Ｈ０４Ｌ	9/00	６７３Ｄ
					６７５Ｄ

Ｆターム(参考) 5B049 BB11 EE05 EE08 GG10
5B055 EE17 HA12 HB04
5B085 AE08 AE25
5J104 AA07 AA09 AA16 EA04 JA21
KA01 KA17 LA03 LA05 LA06
MA01 NA02 NA12 NA36 NA37
NA38 NA42

Ref 1

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-055959

(43)Date of publication of application : 20.02.2002

(51)Int.Cl. G06F 15/00 G06F 17/60
G09C 1/00 H04L 9/32

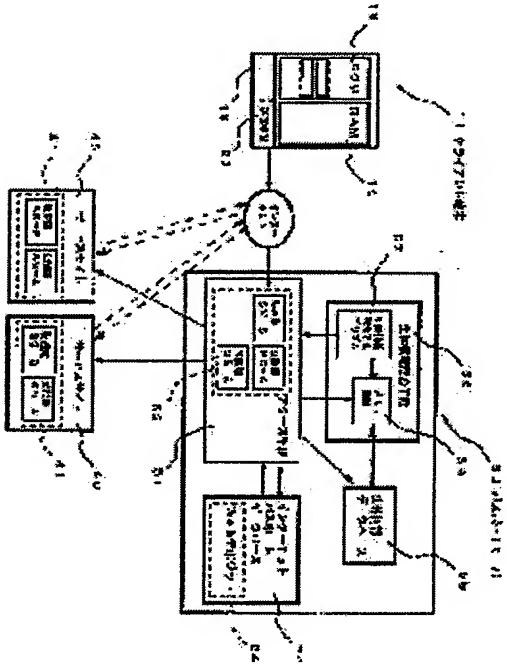
(21)Application number : 2000-243787

(22)Date of filing : 11.08.2000

(71)Applicant : MACKPORT BIO-SECURITY CORP

(72)Inventor : NAKANO YUJI

(54) INFORMATION TERMINAL AND SYSTEM AND METHOD FOR AUTHENTICATION



(57)Abstract:

PROBLEM TO BE SOLVED: To provide a system and a method for authentication with high security which makes it possible to easily and absolutely authenticate a specific person only with a single sign using living body information and disables others to illegally use the living body information.

SOLUTION: This authentication system 10 which manages information regarding the specific person through a network and authenticates whether or not a person accessing the information is the specific person is equipped with a living body information read means 12 which reads the living body information, a living body information registering means 55 which registers the living body information on the specific person for matching, a living body information matching means 56 which matches the pieces of living body information read by the living body information registering means 55 and living body information read means 12 with each other, a passport information storage means 54 which stores pieces of passport information of respective service sites 40 so that they correspond to pieces of living body information registered in the living body information registering means, and an access means 51 which takes corresponding passport information out of the passport information storage means 54 when the pieces of living body information match each other and access the corresponding service site 40.